User Manual

NetProwler™

Version 3.0

The information in this document is subject to change without notice and must not be construed as a commitment on the part of AXENT Technologies. AXENT Technologies assumes no responsibility for any errors that may appear in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such a license.

No part of this documentation may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means—graphic, electronic, or mechanical, including photocopying and recording—without the prior written permission of the copyright owner. The documentation contains confidential and proprietary information of AXENT Technologies, Inc.

© 1999 AXENT Technologies, Inc.
All rights reserved.
Printed in the United States of America.

Additional copies of this document or of other AXENT Technologies publications may be ordered through your AXENT account manager at:

AXENT Technologies, Inc.
2400 Research Blvd., Suite 200
Rockville, MD 20850
Phone: (301) 258-5043
World Wide Web: http://www.axent.com

Technical Support in the United States	**Phone:**	**(801) 227-3700**
	Fax:	**(801) 227-3788**
	E-mail:	**support@axent.com**
For Technical Support in Europe	**Phone:**	**+44 (0) 1372 214321**
	Fax:	**+44 (0) 1372 214341**
	E-mail:	**support@axent.co.uk**
Licensing Issues:	**Phone:**	**(888) 584-3925**
	Fax:	**(781) 487-9818**
	E-mail:	**license@axent.com**

Revison History: May 25, 1999

Trademarks

The AXENT Technologies and the AXENT logo are trademarks of AXENT Technologies, Inc. in the U.S.A. and certain other countries.

Raptor and Raptor Firewall are registered Trademarks of AXENT Technologies, Inc.

NetProwler, Stateful Dynamic Signature Inspection (SDSI), and Intruder Alert are trademarks of AXENT Technologies, Inc.

Intel is a registered trademark, and 386 and 486 are trademarks of Intel Corporation.

Microsoft, Windows, Windows NT, the Windows Logo, and MS-DOS are registered trademarks of Microsoft Corporation.

AIX is a trademark of International Business Machines Corporation.

AXP is a trademark of Digital Equipment Corporation.

HP-UX is a trademark of Hewlett-Packard Company.

IBM is a trademark of International Business Machines Corporation.

Linux is a registered trademark of Linus Torvalds.

OSF is a trademark of Open Software Foundation, Inc.

Solaris, SPARC, and Sun OS are trademarks of Sun Microsystems, Inc.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company, Ltd.

Oracle is a registered trademark of Oracle Corporation.

Internet Scanner is a trademark of Internet Security Systems, Inc.

Firewall-1 is a registered trademark of Check Point Software Technologies, Ltd.

Open Platform for Secure Enterprise Computing (OPSEC) is a trademark of Check Point Software Technologies, Ltd.

All other brands and product names are trademarks or registered trademarks of their respective companies.

Contents

Part A: Getting Started

Chapter 1: Introducing NetProwler

Overview 1.1
Understanding NetProwler 1.2
NetProwler Features 1.3
- Attack Signature Detection 1.4
- Dynamic Attack Signature Definition 1.5
- Network Profiling 1.5
- Live Network Session Monitoring 1.6

File Consistency Checking 1.7
Network Access Restriction 1.8
- Attack Responses 1.9
- Report Generation 1.10
  - Attack Details Report 1.10
  - Executive Summary 1.11
  - Cost Analysis 1.11

In This Manual 1.12

Chapter 2: Installing NetProwler

Overview 2.1
Installation Requirements 2.2
- System Requirements 2.2
- Network Requirements 2.3
- Licensing Requirements 2.3

Deploying NetProwler 2.3
In a De-militarized Zone (DMZ) 2.5
Behind an Internet Firewall 2.6
In a Server Farm 2.6
On a Switched Network 2.6
Installing NetProwler 2.8
Uninstalling NetProwler 2.11
Upgrading NetProwler 2.13

Chapter 3: Touring NetProwler

Overview 3.1
Starting the NetProwler Tour 3.2
Starting the NetProwler Console 3.2
The NetProwler Console 3.4
Menu Bar 3.6
File Menu 3.6
Administration Menu 3.6
Tools Menu 3.7
Windows Menu 3.7
Help Menu 3.7
The Toolbar 3.8
The Configure Tree and Pane 3.9
Attack Branch 3.10
Custom Attacks 3.11
Attack Signature Definition Toolkit 3.12
Profiler Branch 3.16
Scheduling the Profiler 3.18
Consistency Branch 3.18
Conversations Branch 3.20
Access Branch 3.21
Reports Branch 3.22
Address Book Branch 3.23
Application Book Branch 3.24
Notification Options Branch 3.25
Network Devices 3.25
Communication Devices 3.26
Associate Priorities 3.27
The Monitor Tree and Pane 3.28
Statistics Branch 3.28
Alerts Branch 3.30

Attack Branch 3.31
Conversations Branch 3.32
Consistency Branch 3.33
Access Branch 3.33
Reports Branch 3.35
Generated Reports Branch 3.35
Query Parameters 3.36
Query Results 3.36
Stopping NetProwler 3.37

Part B:Configuring NetProwler

Chapter 4: Administering NetProwler

Overview 4.1
Updating NetProwler's License 4.2
Changing NetProwler's Administrative Password 4.3
Obtaining and Importing New Attack Signatures from AXENT 4.5
Setting Up NetProwler's Notification Capabilities 4.7
Configuring NetProwler to Page 4.8
Configuring NetProwler to Send E-mail 4.9
Setting Up NetProwler to Notify a Raptor Firewall 4.11
Setting Up NetProwler to Notify a FireWall-1 Firewall 4.14
Configuring FireWall-1 Authentication 4.17
Configuring NetProwler to Send SNMP Traps 4.19
Setting Up Applications 4.21
Adding an Application 4.22
Deleting an Application 4.24
Modifying an Application 4.24
Purging the NetProwler Database 4.25
Deleting Captured Sessions 4.27
Using Online Help 4.28
Entering Help 4.28
Help Conventions 4.29

Chapter 5: Building the Address Book

Overview 5.1
Profiling a Network 5.2
Starting the Profiler 5.3
Configuring a Profiled System 5.6
Removing (Disabling) a Configured System 5.9
Modifying an Attack Signature (from within the Profiler) 5.11
Scheduling the Profiler 5.13
Adding Systems to the Address Book Manually 5.16
Adding a Single System 5.16
Adding a Range of Systems 5.18
Deleting Systems from the Address Book 5.19

Chapter 6: Configuring NetProwler to Detect Attacks

Overview 6.1
Understanding Attack Signatures 6.2
Common Attacks Signatures 6.2
Port Scan 6.3
SYN Flood 6.3
Denial of Service 6.4
TCP/IP Spoofing 6.4
Ping of Death 6.5
Man in the Middle 6.6
Custom Attacks Signatures 6.7
User-defined Attack Signatures 6.8
Modifying Common Attack Signatures 6.8
Adjusting the Port Scan Threshold 6.8
Adjusting the SYN Flood Threshold 6.9
Adjusting the Denial of Service Threshold 6.9
Adjusting the TCP/IP Spoofing Settings 6.10
Adjusting the Ping of Death Settings 6.12
Associating Attack Signatures Manually 6.13
Disassociating an Attack Signature 6.16
Deleting an Attack Signature 6.18
Changing an Attack Signature's Priority Level 6.18
Configuring NetProwler Actions 6.19
Configuring Notification Actions by Priority Level 6.22
Configuring Response Actions by Attack Signature 6.24

Chapter 7: Creating Attack Signatures

Overview 7.1
The Attack Signature Development Process 7.2
Generate and Collect Data 7.3
Analyze the Data 7.4
Create the Attack Signature 7.4
Test and Debug the Attack Signature 7.5
Understanding the Attack Signature Definition Tool 7.5
The General Tab 7.8
Name and Description 7.8
Attack Signature Types 7.9
Attack Signature Properties 7.12
Applicable Operating Systems and Applications 7.13
The Expressions Tab 7.14
Search Primitives 7.14
Value Primitives 7.17
Reserved Keywords 7.19
Operators 7.26
Building Expressions 7.28
Using Single Primitives or Reserved Keywords 7.28
Creating Simple Expressions 7.28
Creating Complex Expressions 7.29
Setting the Network Frame Direction 7.31
Creating an Attack Signature 7.32
Using the Attack Signature Definition Wizard 7.35
Attack Signature Tutorials 7.39
Creating a Data-specific (FTP) Attack Signature 7.40
Prerequisites 7.41
Creating a Network-specific (LAND) Attack Signature 7.45
Prerequisites 7.45
Creating a Counter-based (Failed Logins) Attack Signature 7.49
Prerequisites 7.49

Chapter 8: Securing Network Resources

Overview 8.1
Securing Web Server Resources 8.2
Modifying a Web Server Consistency Check Entry 8.5

Deleting a Web Server Consistency Check Entry 8.6
Securing FTP Server Resources 8.7
Modifying an FTP Server Consistency Check Entry 8.9
Deleting an FTP Server Consistency Check Entry 8.11
Securing DNS Hostnames 8.12
Modifying a DNS Host Name Entry 8.14
Deleting a DNS Consistency Check Entry 8.15
Securing Router Configuration Files 8.16
Modifying a Router Consistency Check Entry 8.18
Deleting a Router Consistency Check Entry 8.19
Limiting Access to Network Resources 8.20
Modifying a Limit Access Entry 8.22
Deleting a Limit Access Entry 8.24

Chapter 9: Monitoring Attacks and Network Conversations

Overview 9.1
Monitoring Attacks that NetProwler Detects 9.2
    Viewing All Alerts 9.2
    Resetting Alerts 9.3
    Viewing Alerts by Attack Type 9.4
    Viewing Captured Attack Sessions 9.5
Configuring Conversation Monitoring 9.5
Viewing Live Conversations 9.7
Terminating Conversations 9.8
Capturing Conversations 9.9
Viewing Captured Conversations 9.11

Chapter 10: Generating and Viewing Reports

Overview 10.1
Scheduling Reports 10.2
    Executive Summary 10.2
    Cost Analysis 10.5
    Attack Details 10.8
Modifying Scheduled Reports 10.11
    Viewing and Modifying Currently Scheduled Reports 10.11
    Deleting a Scheduled Report 10.12
    Turning Off Scheduled Reports 10.12
Viewing Reports 10.13

Viewing HTML Reports 10.13
Viewing CSV and TSV Reports 10.14
Deleting Reports 10.14
Generating User-defined Reports 10.15
Saving a User-defined Report 10.17

Appendices

Appendix A: Getting Help

Overview A.1
Online Help A.2
User and Installation Manuals A.3
Release Notes A.3
Online Support Services A.4
Training A.5
Tradeshows A.6
Technical Support A.7
Before Contacting Technical Support A.7
Console Information A.8
Network Information A.8
Problem Information A.9
Contacting Technical Support A.10
United States A.10
Europe A.10
Licensing A.10
World Wide Web site A.10
Anonymous FTP A.10
AXENT Consulting Services A.11
Links to Other Security Resources A.12

Appendix B: Optimizing NetProwler's Performance

Overview B.1
Monitoring NetProwler's Performance B.2
Improving NetProwler's Performance B.3

Appendix C: Attack Signature Descriptions

Overview....C.1
NetProwler's Predefined Attack Signatures....C.2
- Apache_Web_Server_Denial_of_Service_Attack....C.2
- ARP_Host_Down_Check....C.2
- ASCEND_ROUTE_ASCEND_KILL....C.3
- BackOrifice_Detect....C.3
- Bonk_Attack....C.3
- Brute_Force_Login_Attempt....C.4
- Cookie_Monster_Attack_Decode....C.4
- DIG_Attack....C.5
- DNS_REQUEST_BROADCAST....C.5
- DNS_Zone_Transfer_Decode....C.6
- Duplicate_IP_Address_Detection....C.6
- Echo_Chargen_loop_Attack....C.7
- E-mail_From_Decode....C.7
- E-mail_To_Decode....C.8
- Finger_User_Decode....C.8
- FTP_CWD_Vulnerability....C.8
- FTP_Get_File_Decode....C.9
- FTP_MKDIR_Decode....C.9
- FTP_Password_Decode....C.10
- FTP_PUT_Decode....C.10
- FTP_RMDIR_Decode....C.11
- FTP_Root_User_Access_Decode....C.11
- FTP_Scan....C.12
- FTP_SITE_EXEC_Vulnerability....C.12
- FTP_SITE_Vulnerability....C.13
- FTP_USER_Decode....C.13
- FTP_Arg_Core_Dump_Decode....C.14
- HP_UX_NETTUNE_Attack....C.14
- HP_UX_PPL_EXPLOIT_Attack....C.15
- HPUX_RemoteWatch_Vulnerability....C.15
- HTTP_Campas_CGI_Vulnerability....C.16
- HTTP_Convert_CGI_BIN_Vulnerability....C.16
- HTTP_Glimpse_Vulnerability....C.17
- HTTP_Java_Decode....C.17
- HTTP_NPH_TEST_Vulnerability....C.18

HTTP_PHF_CGI_Vulnerability C.18
HTTP_SGI_Wrap_Vulnerability C.19
HTTP_TEST_Vulnerability C.19
HTTP_View_Source_Script_Vulnerability C.20
HTTP_BAT_FILE_EXEC C.20
HTTP_COUNT_CGI_DECODE C.20
HTTP_ETC_PASSWD_DECODE C.21
HTTP_EXEC_ISP_FILE C.21
HTTP_UPLOADER_DECODE C.22
HTTP_WIN_C_SAMPLE_DECODE_ASD C.22
ICMP_Dst_Proto_Unreachable_Decode C.23
ICMP_Redirect_Host_Redirect_Message C.23
ICMP_Redirect_Net_Redirect_Message C.24
ICMP_Redirect_Packet C.24
ICMP_Redirect_TOS_Host_Redirect_Message C.25
ICMP_Redirect_TOS_Net_Redirect_Message C.25
ICMP_SMURF C.26
IDENT_Newline_Vulnerability C.26
IDENT_User_Decode C.27
IMAP_Username_Password_Decode C.27
INVALID_TCP_FRAME_DETECT C.28
INVALID_TTL_DECODE C.28
IP_Options_Loose_Source_Routing_Decode C.29
IP_Options_Record_Route_Decode C.29
IP_Options_Security_Enabled_Decode C.30
IP_Options_Strict_Source_Routing_Decode C.30
IP_Options_TimeStamp_Decode C.31
IP_Unknown_Protocol C.31
IRC_Channel_Decode C.32
IRC_Message_Decode C.32
IRC_Nick_Decode C.32
LAND C.33
LATIERRA C.33
LINUX_Dump_Command_Vulnerability C.33
LINUX_KBD_Denial_of_service C.34
LINUX_Login_Command_Vulnerability C.34
LINUX_Login_Vulnerability C.35
LINUX_LOGIC_BOMB_Attack C.35
LINUX_SHADOW_FILE_Attack C.36

MICRO_FRAGMENT_DETECT C.36
MS_IE_LNK_Vulnerability C.37
MS_IE_URL_Vulnerability C.37
MS_WIN_Remote_Passwd_Access C.37
MS_WIN_Remote_Registry_Access C.38
MS_IIS_ASP_Attack C.38
MS_JOLT_Attack C.38
MS_WIN_SAM_ACCESS C.39
Netscape_Cache_Cow_Attack_Decode C.39
Netscape_Son_Of_Cache_Cow C.39
NewTear C.40
NFS_EXPORT_Command_Decode C.40
NNTP_Group_Decode C.40
NNTP_Password_Decode C.41
NNTP_Username_Decode C.41
NT_DNS_QR_Bit_Vulnerability C.41
NT_IIS_Telnet_GET_Vulnerability C.42
NT_PortMapper_Flood C.42
NT_Telnet_denial_of_service C.42
NT_DNS_Attack C.42
OOB_Attack_ON_NT C.43
PING_REPLY_FLOOD C.43
POP_Password_Decode C.44
POP_Username_Decode C.44
Remote_Packet_Capture_Decode C.45
RLogin_Vulnerability_Attack C.45
SMTP_DEBUG_Decode C.46
SMTP_EXPN_Decode C.46
SMTP_Piped_Command_Vulnerability C.47
SMTP_QMAIL_Vulnerability C.47
SMTP_VRFY_Decode C.48
SMTP_WIZ_Decode C.48
SunOS_UDP_Bomb C.49
SunOS_AUDIOOCTL_KERNEL_PANIC C.49
SunOS_dev_nit_exploit C.50
SunOS_DF_Attack C.50
SunOS_Keyboard_Kernal_Panic C.51
SunOS_Not_On_System_Console C.51
SunOS_Ping_Crash_Attack C.51

SunOS_TCP_Kernal_Panic C.52
SunOS_TCX0_Kernal_Panic C.52
SynDrop C.53
Syslog_fogger C.53
TearDrop C.54
Telnet_detect C.54
Telnet_Potential_Denial_of_Service C.54
TFTP_GET_Vulnerability C.55
TFTP_PUT_Vulnerability_Attack C.55
TRIPWIRE_Attack C.56
UDP_Scan C.56
UDP_SMURF C.57
UNIX_Finger_Access_Decode C.57
UNIX_Finger_Bomb_Vulnerability C.58
UNIX_Hosts_File_Access C.58
UNIX_Rhost_File_Access C.59
UNIX_Home_Change_Mode_Vulnerability C.60
UNIX_Mail_Change_Mode_Vulnerability C.60
UNIX_ADM_Messages_Attack C.61
UNIX_Aliases_Dir_Attack C.61
UNIX_Aliases_Pag_File_Attack C.62
UNIX_Bliss_Virus_Attack C.62
UNIX_CULOG_File_Attack C.63
UNIX_Errorlog_File C.63
UNIX_ETC_Exports_File_Attack C.64
UNIX_ETC_Host_File_Attack C.64
UNIX_ETC_Inetd_Conf_File_Attack C.65
UNIX_ETC_Utmp_File_Attack C.65
UNIX_Host_Equiv_File_Attack C.66
UNIX_Loginlog_File_Attack C.66
UNIX_Passwd_File_Attack C.67
UNIX_Sulog_File_Attack C.67
UNIX_Var_Adm_Lastlog_File_Attack C.68
UNIX_XLOCK_Vulnerability C.68
Winnuke C.69
WS_FTP_INI_Attack C.69
X_Server_Crash_Attack C.69

List of Figures

1-1: Network Intrusion Detection with NetProwler 1.2
1-2: Profiler Start Scan Dialog Box 1.5
2-1: NetProwler Coverage 2.4
2-2: NetProwler Installations 2.5
2-3: Installing on a Switched Network 2.7
2-4: NetProwler Welcome Screen 2.8
2-5: Adaptor List Dialog Box 2.9
2-6: Select Destination Directory Dialog Box 2.10
2-7: Uninstalling the NetProwler Application Dialog Box 2.11
2-8: NetProwler Welcome Screen 2.14
2-9: NetProwler Install Found Dialog box 2.15
3-1: NetProwler Authentication Dialog Box 3.3
3-2: NetProwler Console Elements 3.5
3-3: Configure Tree Branches and Objects 3.9
3-4: Attack Branch Objects 3.10
3-5: Port Scan List in the Configure Pane 3.11
3-6: Pre-defined Attack Definition list 3.11
3-7: Attack Signature Definition Dialog Box 3.12
3-8: Attack Signature Dialog Box -Expressions Tab 3.13
3-9: Custom Attack Association List 3.13
3-10: Edit Attack Associations Dialog Box 3.14
3-11: Edit Attack Association Details dialog box 3.15
3-12: Start Scan Dialog Box 3.16
3-13: Profiler Results Screen 3.17
3-14: Profiler Schedule Dialog Box 3.18
3-15: Consistency Branch 3.19
3-16: Consistency Check List 3.19
3-17: Conversation Branch 3.20
3-18: Access Branch 3.21
3-19: Reports List in the Configure Pane 3.22
3-20: NetProwler Address Book List 3.23
3-21: Application Book Branch 3.24
3-22: Notification Options Branch 3.25
3-23: Pager Options - Communication Devices Branch 3.26
3-24: E-mail Options - Communication Options Branch 3.27
3-25: Associate Priorities Options 3.27
3-26: Statistics Branch in the Monitor Tree 3.28
3-27: Alerts and Protocol Distribution Graphs 3.29
3-28: Frame Statistics Counter 3.29

3-29: Alerts Branch 3.30
3-30: Attacks Branch 3.31
3-31: Conversations Branch 3.32
3-32: Consistency Branch 3.33
3-33: Web Server Consistency Check 3.33
3-34: Access Branch -Time Access Limits 3.34
3-35: Reports Branch 3.35
3-36: Generated Reports 3.35
3-37: Query Parameters 3.36
3-38: NetProwler Authentication Dialog Box 3.37
4-1: NetProwler Authentication Dialog Box 4.3
4-2: Select Attack Signature File Dialog Box 4.6
4-3: Pager Options Box 4.8
4-4: E-mail Options Box 4.9
4-5: Notifying a Raptor Firewall 4.11
4-6: Firewall Options Box 4.13
4-7: Notifying a Firewall 4.15
4-8: Firewall Options Box 4.16
4-9: SNMP Box 4.20
4-10: Application Book Entry Dialog Box 4.22
4-11: Edit Application Book Entry Dialog Box 4.25
4-12: Purge Database Dialog Box 4.26
4-13: NetProwler Information Dialog Box 4.26
5-1: Start Scan Dialog Box 5.4
5-2: NetProwler Dialog Box 5.6
5-3: Host Details Dialog Box 5.7
5-4: Edit Attack Associations Dialog Box 5.8
5-5: Profiler Schedule Dialog Box 5.14
5-6: Address Book Entry Dialog Box 5.17
5-7: Address Book Entry Dialog Box 5.18
6-1: TCP Three-way Handshake 6.3
6-2: Man-in-the-Middle Attack Diagram 6.6
6-3: Port Scan Threshold Settings 6.8
6-4: SYN Flood Threshold Settings 6.9
6-5: Denial of Service Threshold Settings 6.10
6-6: TCP/IP Spoofing Dialog Box 6.11
6-7: Port Scan Threshold Settings 6.12
6-8: Edit Attack Association Dialog Box 6.14
6-9: Edit Attack Association Details 6.15
6-10: Edit Attack Association Dialog Box 6.17

6-11: The Priority Configuration Boxes 6.23
6-12: Edit Attack Association Details Dialog Box 6.25
7-1: Attack Signature Development Process 7.2
7-2: Attack Signature Definition Dialog Box (General Tab) 7.6
7-3: Attack Signature Definition Dialog Box (Expression Tab) 7.7
7-4: Applies To Box 7.13
7-5: Search Primitives Tab 7.14
7-6: Value Primitives Tab 7.17
7-7: Reserved Keywords Tab 7.20
7-8: Form of Simple Expressions 7.28
7-9: Forms of Complex Expressions 7.29
7-10: Attack Signature Definition Dialog Box 7.33
7-11: Expressions Tab 7.34
7-12: Search Primitive Creation Dialog Box 7.36
7-13: Attack Signature Template Dialog Box 7.37
7-14: Attack Association Dialog Box 7.38
7-15: FTP Host Configuration 7.40
7-16: Attack Signature Definition Dialog Box 7.42
7-17: Search Primitive Tab 7.43
7-18: Expression box 7.44
7-19: Attack Signature Definition Dialog Box 7.46
7-20: Expressions Tab 7.47
7-21: Attack Signature Definition Dialog Box 7.50
7-22: Expressions Tab 7.51
7-23: Expression Box 7.52
8-1: Web Consistency Check dialog box 8.3
8-2: Edit Web Server Consistency Check Dialog Box 8.5
8-3: FTP Consistency Check Dialog Box 8.8
8-4: Edit FTP Server Consistency Check Dialog Box 8.10
8-5: DNS Consistency Check Dialog Box 8.12
8-6: Edit DNS Consistency Checking Dialog Box 8.14
8-7: Router Consistency Check Dialog Box 8.17
8-8: Edit DNS Consistency Checking Dialog Box 8.18
8-9: New Time of Day Access Entry 8.21
8-10: Edit Host Entry Dialog box 8.23
9-1: Monitor Pane - Port Scan Attack 9.4
9-2: Capture Session To File dialog box 9.10

10-1: The Schedule Reports Entry dialog box. 10.3
10-2: The Schedule Reports Entry dialog box. 10.6
10-3: The Schedule Reports Entry dialog box. 10.9
10-4: Query Options 10.15
A-1: Online Help A.2
B-1: Frame Statistics and Protocol Distribution B.2

List of Tables

4-1: Application Type Description 4.23
4-2: Help Tab Descriptions 4.28
4-3: Conventions Used in Online Help 4.29
5-1: Modification Options 5.12
6-1: TCP/IP Spoofing Types 6.11
6-2: Modification Options 6.15
6-3: Notification Actions 6.20
6-4: Response Actions 6.20
6-5: Configuration Options 6.21
6-6: Priority Levels Defined 6.22
7-1: Attack Signature Types 7.9
7-3: Search Primitive Options 7.15
7-4: Value Primitive Options 7.17
7-5: Reserved Keywords—Protocols 7.20
7-6: Reserved Keywords—IP Header 7.21
7-7: Reserved Keywords—ICMP Header 7.23
7-8: Reserved Keywords—UDP Header 7.24
7-9: Reserved Keywords—TCP Header 7.24
7-10: Logical Operators 7.26
7-11: Bit-wise Operators 7.26
7-12: Equality Operators 7.27
7-13: Arithmetic Operators 7.27
7-14: Combination Operators 7.27
10-1: Query Options 10.16
A-1: Required GUI Information A.8
A-2: Required Network Information A.8
A-3: Required Problem Information A.9

Getting Started

Chapter 1: Introducing NetProwler

Chapter 2: Installing NetProwler

Chapter 3: Touring NetProwler

Introducing NetProwler

Overview

NetProwler™ provides dynamic network intrusion detection by transparently examining network traffic to detect, identify, log, and terminate unauthorized use or misuse of computer systems.

NetProwler is the only network-based Intruder Detection System (IDS) that combines “out of the box” use, attack signature extensibility, real-time signature deployment, and multi-platform host IDS integration.

The need for NetProwler is paramount in an era characterized by complex computing environments, vast conglomerates of integrated computer networks, and increasing computer-related crime.

This chapter provides an overview of NetProwler including how NetProwler detects and responds to network-based attacks. Chapter topics include:

- Understanding NetProwler
- NetProwler Features
- In This Manual

Understanding NetProwler

NetProwler monitors network traffic for suspicious behavior and responds to intrusion attacks in real time. By monitoring the network traffic between servers, clients, and other network devices, NetProwler detects network-oriented attacks, such as TCP/IP spoofing and SYN flooding.

NetProwler installs on a single dedicated computer connected to an Ethernet 10 Mbps or 100 Mbps network using the TCP/IP communication protocol suite—hereafter referred to as simply TCP/IP. Because NetProwler resides on a dedicated server, it can detect network attacks without impacting the performance or accessibility to other networked systems or devices. It is completely transparent to users on the network. Figure 1-1 illustrates how NetProwler sits on the network monitoring all TCP/IP traffic on the network segment.

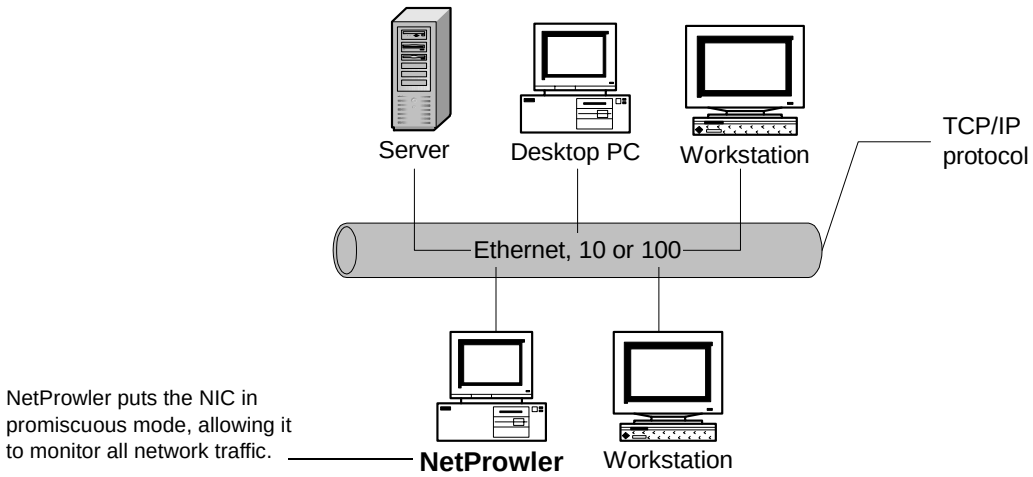


Figure 1-1: Network Intrusion Detection with NetProwler

NetProwler works by placing the system's network interface card (NIC) in "promiscuous" mode. This allows it to monitor the TCP/IP traffic it can see. NetProwler detects sophisticated attacks by comparing packet data to its database of attack signatures. An attack signature is a set of rules that define a set of actions that identify an attacker's attempt to exploit a known operating system or application vulnerability. An attack

signature may identify a series of commands, a communication pattern, or a sequence of communication patterns between two network devices. When NetProwler detects an attack signature, it displays a flashing light icon in the NetProwler console to notify you of the attack. You can then look in the Alerts branch in the Monitor tree to determine the type of the attack. Once you know the type of attack, you can click on it in the Attacks branch to view specific details such as the attacked system, attacking system, and time of the attack. In addition to logging the alarm in the console, NetProwler performs all other configured actions. Available actions include:

- Resetting the attacker's session
- Capturing the session
- E-mail an administrator
- Page an administrator
- Spawn a command or batch file
- Send SNMP traps
- Harden a firewall

NetProwler Features

NetProwler provides the following major features that make network intrusion detection convenient and efficient:

- Attack signature detection
- Dynamic attack signature definition
- Network profiling (scanning)
- Live network session monitoring
- File consistency checking
- Attack responses
- Report generation

Each feature is described in the paragraphs that follow.

Attack Signature Detection

NetProwler's exclusive, patent-pending technology uses an advanced method of detection called Stateful Dynamic Signature Inspection™ (SDSI™) to detect network-based attacks.

Stateful means that NetProwler can remember the contents of the active sessions that it monitors on the network. Therefore, rather than simply comparing an attack signature with a single packet, NetProwler builds a context around a network session. This allows NetProwler to monitor and prevent much more sophisticated attacks than the simple exploits that a single packet of data may contain. For example, NetProwler can detect attacks that occur in separate actions or steps.

Dynamic means that you can create new attack signatures and have them activated in real time, without having to take the system offline. In addition, this technology allows you to customize NetProwler to your organization's needs and respond to the threats that your organization faces.

Signature Inspection is the method of detection that NetProwler uses. Signature Inspection works by comparing an attack signature (a set of rules that describe an attack) to a communication packet.

NetProwler comes with numerous predefined operating system and application attack signatures that can be enabled quickly for individual hosts and ranges of hosts. It contains attack signatures for many well-known internet attacks including Ping of death, SYN Flood, and TCP/IP spoofing. For a list and description of the attack signatures that shipped with this version of NetProwler, see *Appendix C: Attack Signature Descriptions*.

For information on configuring NetProwler's attack signature definitions, see *Chapter 6: Configuring NetProwler to Detect Attacks.*

Dynamic Attack Signature Definition

In addition to the predefined attack signatures that come with NetProwler, NetProwler's Attack Signature Definition toolkit empowers you with the ability to create new, custom attack signatures that address company specific resources and applications. NetProwler's Attack Signature Detection tool uses SDSI technology. This lets you detect suspicious activity, monitor the activity, define new attack signatures, and activate the signatures to stop new instances of the attack without any interruptions in monitoring. For information on downloading or creating new attack signatures, see *Chapter 7: Creating Attack Signatures.*

Network Profiling

NetProwler provides an automated configuration tool called the "Profiler." The Profiler scans the network for "live" systems, and guides you through the process of defining which systems you want to monitor and what attack signatures you want associated with each system.

The Profiler offers the most efficient and convenient means of configuring NetProwler. Figure 1-2 illustrates the Profiler's Start Scan dialog box. (The Start Scan dialog box is used to configure and initiate the Profiler.)

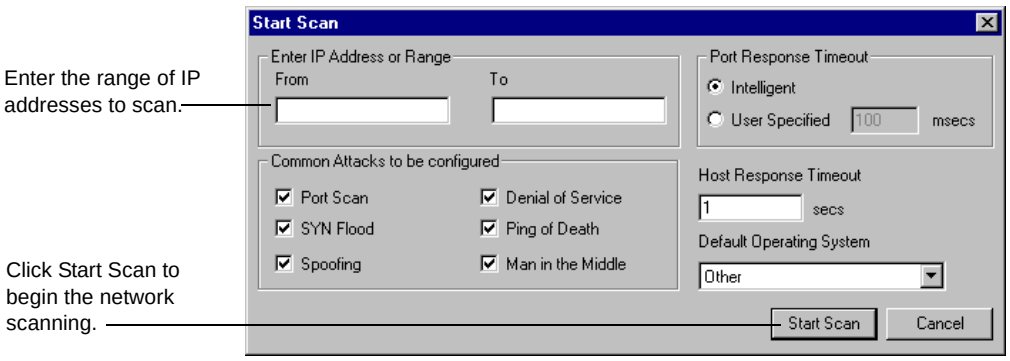


Figure 1-2: Profiler Start Scan Dialog Box

After specifying the range of IP addresses to scan, checking the Common attack signatures, and configuring the time out parameters, click Start Scan. As the Profiler scans the network for live systems within the specified range of IP addresses, it also scans the well-known ports on live systems to see what services are available. NetProwler uses this information to intelligently recommend or automatically apply the appropriate attack signatures.

When the Profiler completes the scanning process, you can enable each detected host with the desired attack signatures. Then you can add the systems to the Address Book for NetProwler to monitor.

In addition, the Profiler's scheduling feature allows you to keep NetProwler configured as your network configuration changes. The scheduling feature automatically rescans the network at specified intervals (e.g., each day, week, or month) to discover new systems or systems that were not live during previous scans. The Profiler's scheduling feature automatically keeps NetProwler up-to-date on your network's latest configuration changes. For more information on the Profiler, see *Chapter 5: Building the Address Book*.

Live Network Session Monitoring

NetProwler features live network session monitoring and capturing. NetProwler can monitor TCP/IP session types, such as ftp, telnet, and HTTP, as they occur in real time.

With the click of a button, you can look at session details as the session transpires in real time. For example, when viewing a telnet session, you can see the commands that the client system sends to the server. NetProwler receives the data transmitted over the network in its raw form, automatically attempting to decode it as text for display. On these application sessions, you can view the user's entries and the server's responses in real time.

Some applications such as HTTP use a number of different sessions to exchange data. NetProwler does not display each and every communication, for example every *GET* request. In those cases, NetProwler displays a virtual session to indicate that the client and server are communicating.

NetProwler's network session monitoring feature also contains two other convenient options: Capture and Terminate.

Capture lets you capture a suspicious network session to a file for review at a later time. You can replay the captured file and use it to create new attack signatures.

Terminate lets you immediately respond to an attack by terminating the network session.

For more information on NetProwler's live network monitoring feature, see *Chapter 9: Monitoring Attacks and Network Conversations*.

File Consistency Checking

NetProwler's Consistency Checking feature monitors important network resources. It works by comparing web server and ftp server configuration files on a byte-by-byte basis with files on a mirrored site. NetProwler also checks DNS hostname and router configuration files to ensure that they have not been modified without authorization and displays the results of the consistency check in the Monitor pane. NetProwler's Consistency Checking feature can monitor:

- **DNS Entries.** NetProwler can monitor changes to your DNS table. NetProwler tests the DNS hostnames at periodic intervals to ensure that they have not been remapped to unwanted IP addresses. This lets you detect malicious actions such as an attacker changing a world wide web (www) hostname to the web server of a competitor.

- **Router Configuration Tables.** NetProwler can monitor a router's configuration table. This can help detect denial of service attacks such as an attacker changing the routing of network traffic to an invalid gateway.
- **Web Server Files.** NetProwler can monitor static information, such as HTML pages, scripts, or images on a web site, and compare it against the corresponding information on a mirrored site. This helps ensure that files have not been modified or corrupted by an attack.
- **FTP Server.** NetProwler can monitor files or directories on an FTP server and compare them on a byte-to-byte basis against an FTP mirror site. This lets you ensure that files that can be downloaded publicly have not been infected with viruses or replaced by different files with the same name.

For more information on file consistency checking, see *Chapter 8: Security Network Resources.*

Network Access Restriction

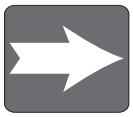
NetProwler lets you stop traffic to one or more TCP/IP based applications on a monitored system. You can limit traffic to one or more systems on the network during certain times of the day or certain days of the week. NetProwler can perform this function without modifying client or server workstations.

You can use NetProwler's limit access feature when network services are provided for internal use only. For example, access to an intranet FTP server that contains sensitive information can be restricted to weekdays. Once you create a time access entry, you can modify or delete the entry when necessary.

Attack Responses

You can configure NetProwler to take actions in response to an attack using one or all of the following *notification* actions:

- E-mail an Administrator
- Page an Administrator
- Reconfigure a firewall
- Send SNMP Traps



You can integrate NetProwler with Intruder Alert by sending SNMP Traps to an Intruder Alert Agent. This allows you to take advantage of Intruder Alert's response mechanisms, such as disable an account, raise global flags, start timers, and send on-screen notification to remote hosts. For instructions on how to configure Intruder Alert to receive and respond to SNMP traps, see the *NetProwler-Intruder Alert Integration Manual* that shipped with the NetProwler CD-ROM.

Additionally, you can configure NetProwler to respond to some custom attacks with one or more of the following *response* actions:

- Capture the attack session
- Reset the session
- Spawn a command

You can configure NetProwler to respond to an attack globally by priority or individually by attack signature. If an attack signature's notification actions differ from those configured by priority level, then the actions configured by attack signature take precedence.

For more information on configuring attack notifications and responses, see *Chapter 6: Configuring NetProwler to Detect and Monitor Attacks*.

Report Generation

You can use NetProwler's report generation feature to generate three different types of reports:

- Attack Details
- Executive Summary
- Cost Analysis

You can e-mail reports to an administrator or generate HTML reports for viewing in a web browser.

Attack Details Report

The Attack Details report describes attacks that have taken place during a defined time period. You can configure NetProwler to report at hourly, daily, weekly, or monthly intervals. You can even schedule reports at shorter intervals, such as five or ten minutes.

The Attack Details report provides the following information for each type of alarm selected:

- Attacked Host
- Attacking Host
- Attack Type
- Attack Time
- Attack Priority

You can choose to generate a report that contains details for a specific type of attack only or generate a report that includes all of the attacks. You can also choose the Summary option to get a graph of all attacks seen during a certain period of time.

The Attack Details report can be generated in comma-separated (CSV), tab-separated (TSV), HTML, and e-mail formats, so that them can be imported into numerous, popular report generation and database applications.

Executive Summary

The Executive Summary report helps you to determine possible security problems by comparing the number of attacks at each priority with the number of attacks that you expected to see. You can configure NetProwler to generate an Executive Summary report at daily, weekly, or monthly intervals.

Cost Analysis

The Cost Analysis report estimates how much an attack might cost you. You provide a value as to how much an unavailable server might cost you and an average of the criticality of the monitored servers. NetProwler then uses those estimates to calculate what an attack during a specified time cost.

For more information on NetProwler reports, see *Chapter 10: Generating and Viewing Reports*.

In This Manual

This section provides a brief introduction to the chapters and appendices contained in this manual.

- *Chapter 1: Introducing NetProwler*

  This chapter provides an overview of NetProwler. It explains how NetProwler works to detect network-based attacks, how it responds to attacks, and the features NetProwler provides.

- *Chapter 2: Installing NetProwler*

  This chapter provides instructions on installing and deploying NetProwler in the enterprise. It includes system and network requirements, installation procedures, deployment considerations, and upgrading procedures.

- *Chapter 3: Touring NetProwler*

  This chapter takes new users on a guided tour of the NetProwler Console. Topics include the features of the graphical user interface and each feature comprising NetProwler. This chapter provides an excellent way for new users to become more familiar with NetProwler.

- *Chapter 4: Administering NetProwler*

  This chapter contains the concepts and instructions for configuring and administering NetProwler. It includes instructions on such tasks as starting the NetProwler Console, updating your NetProwler licensing, setting up response capabilities such as e-mailing or paging an administrator, hardening a firewall, or sending SNMP traps.

- *Chapter 5: Building the Address Book*

  This chapter provides instructions on using the Profiler to identify and configure systems in NetProwler's Address Book. In addition, it describes how to manually configure the Address Book by adding or removing systems.

- *Chapter 6: Configuring NetProwler to Detect Attacks*

  This chapter teaches you how to configure NetProwler to monitor specific hosts, ranges of hosts, network session attacks, and specific applications. Additionally, it provides instructions on how to activate or deactivate attack signatures, and how to configure NetProwler to detect and respond to common network attacks such as Port Scan and Ping of Death.

- *Chapter 7: Creating Attack Signatures*

  This chapter describes attack signatures and explains how to create new attack signatures.

- *Chapter 8: Securing Network Resources*

  This chapter describes how configure NetProwler to monitor web files, ftp files, system files, DNS host tables, and router configuration tables to ensure that intrusion attacks have not changed or corrupted them. It also describes how to use NetProwler to limit access to network resources.

- *Chapter 9: Monitoring Attacks and Network Conversations*

  This chapter teaches you how to use the Monitor pane to view active network sessions, record a network session, replay a session, view events in text mode, and delete a captured session.

- *Chapter 10: Generating and Viewing Reports*

  This chapter describes NetProwler's reports and explains how to schedule reports, view alarms, and query the alarm database.

- *Appendix A: Getting Help with NetProwler*

  This appendix describes where users can turn for help on using NetProwler. Help sources include: online help, user manuals, release notes, AXENT™ Online, product training, customer support, professional services, and online links to other security resources.

- *Appendix B: Optimizing NetProwler's Performance*

  This appendix describes how to monitor NetProwler's performance and suggests ways of optimizing it.

- *Appendix C: Attack Signature Descriptions*

  This appendix lists and describes the predefined attack signatures that shipped with this release.

Chapter 2

Installing NetProwler

Overview

This chapter describes the steps necessary to successfully install and deploy NetProwler on your network. NetProwler installs on Windows NT systems connected to the network segments that you want to monitor. Each network segment that you want to monitor requires a separate installation of NetProwler.

This chapter also contains prerequisites such as system requirements, network type requirements, suggestions on deploying NetProwler in the network, and upgrading procedures.

Chapter topics include:

- Installation requirements
- Deploying NetProwler on the network
- Installing NetProwler on a Windows NT system
- Upgrading procedures

Installation Requirements

NetProwler installs on Windows NT systems. AXENT recommends that the system on which you install NetProwler be dedicated to intrusion detection. You should not use that system to run other applications. If other applications are installed on the same system, both NetProwler and those applications may experience diminished performance. Installing NetProwler on a dedicated server allows it to transparently monitor network-based attacks without impacting performance or accessibility. In addition, it enhances the security of the dedicated system.

System Requirements

The following list defines the minimum system requirements for running NetProwler:

- Windows NT 4.0 server or workstation
- Service Pack 3 or 4 installed
- Pentium or Pentium equivalent (or greater) processor (recommended)
- 64 MB RAM
- 50 MB free hard disk space
- 150 MB of Virtual Memory
- Fully configured TCP/IP stack
- Static IP address, gateway, and DNS entry
- Ethernet 10 or 100 Mbps network interface card
- Modem (optional—used for pager notification)

Additional memory and disk space may be required depending on the number of nodes being monitored, the number of applied attack signatures, and the capacity of the Ethernet network being monitored (10 or 100 Mbps).

Network Requirements

NetProwler requires a network with the following components:

- Network Interface Card (NIC)
- 10- or 100-Base T Ethernet network

Licensing Requirements

NetProwler requires you to enter a 19-character license key during the installation process. Each NetProwler installation requires a separate license key. The license key enables NetProwler to scan an unlimited number of nodes on the segment of the network on which it resides.

Licenses can be acquired by contacting your AXENT account manager, or by e-mailing AXENT's licensing administrator at:

license@axent.com

Deploying NetProwler

To ensure complete coverage of your network resources, you should give careful consideration to the configuration of your network and the placement of your NetProwler installations.

NetProwler works by monitoring communication sessions occurring on the same network segment where it is installed. Therefore, NetProwler can monitor only those systems and devices that communicate over the same network segment where it is installed. Basically, NetProwler can monitor anything that it can see. Networks containing multiple segments connected to each other with various devices such as routers, bridges, hubs, and switches will require multiple installations of NetProwler.

As Figure 2-1 illustrates, one installation of NetProwler monitors network traffic on segment A, while a second NetProwler installation monitors network traffic on segment B.

Each NetProwler installation monitors a specific segment of the network for attack signatures that indicate an intrusion attack.

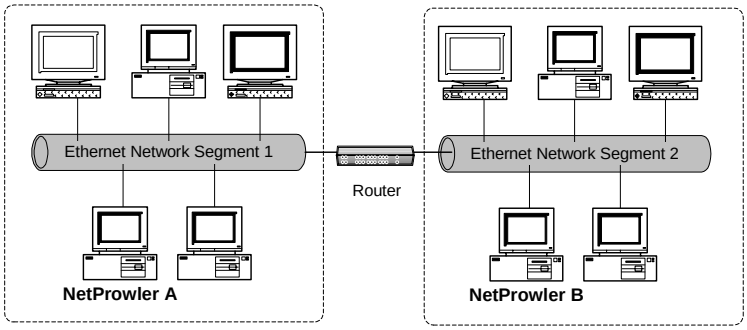


Figure 2-1: NetProwler Coverage

You should install NetProwler on each network segment that contains important resources. The specific segments on which you install NetProwler will depend on your organization's network arrangement and security policy. However, three

locations are particularly important in protecting against intrusion attacks: the de-militarized zone, behind the firewall, and in a server farm. Figure 2-2 illustrates these locations.

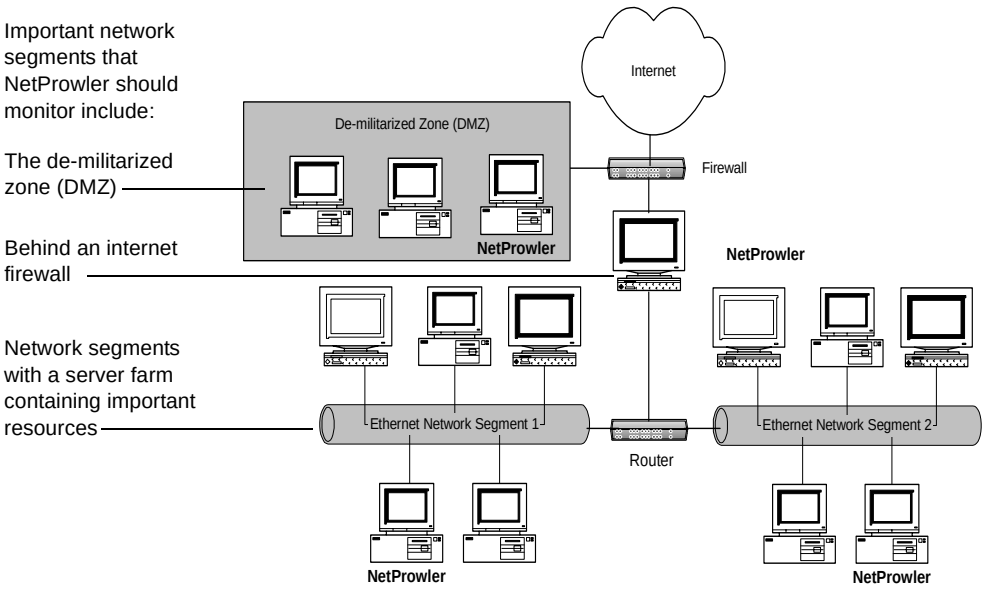


Figure 2-2: NetProwler Installations

In a De-militarized Zone (DMZ)

A de-militarized zone (DMZ), sometimes called a perimeter network, is the segment of the internal network that allows access to external users. It usually contains the company's web and ftp servers and consequently is often the first target for intrusion attacks. The DMZ provides an additional layer of access between the internal network and any external hosts such as those coming in from the Internet.

Installing NetProwler in the DMZ lets you monitor network traffic from both external and internal users when they connect to systems in the DMZ. NetProwler helps you discover and respond to intrusion attacks before they reach your vital internal resources.

Behind an Internet Firewall

Installing NetProwler behind the firewall ensures that all traffic from the internal LAN to the internet and all traffic incoming to the LAN is monitored.

NetProwler monitors traffic coming through the firewall. Many internet firewalls are not capable of detecting attacks such as port scan. Placing NetProwler behind the firewall adds an additional layer of protection and ensures that intrusion attacks that pass through the firewall are detected and responded to.

In a Server Farm

Server farms or any group of servers that contain important company resources should be protected by NetProwler. By placing NetProwler on the same subnetwork as the server farm, you can monitor those servers for intrusion attacks from RAS (remote access services) users, internal abusers, or internet attacks.

You can also define custom attack signatures to protect company-specific applications, such as databases, on specific systems of a server farm

On a Switched Network

Some Ethernet networks use switches or switching hubs. Switched networks provide more network security because they send packets to only their destination systems; other systems on the network do not receive the packets.

Placement of NetProwler installations on switched networks requires careful consideration. The configuration and hardware used in your switched network will determine the placement of NetProwler. In many network configurations this usually means using a monitored port on the switch. Consult your hardware device documentation for details on configuring a monitored

port. You would then install NetProwler on a dedicated system using the monitored port. NetProwler must be able to see the network traffic on the systems that it monitors. The following graphic illustrates a sample installation.

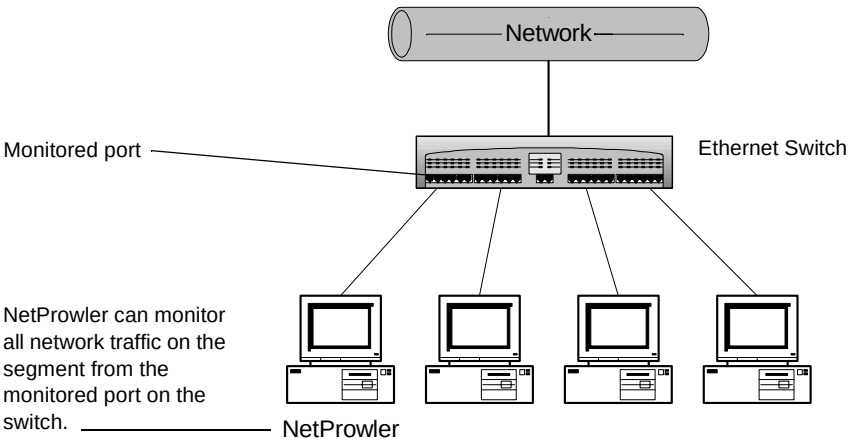

Network
Monitored port
Ethernet Switch
NetProwler can monitor all network traffic on the segment from the monitored port on the switch.
NetProwler

Figure 2-3: Installing on a Switched Network

Installing NetProwler

You must install NetProwler on a Windows NT 4.0 Workstation or Server with either Service Pack 3 or 4 installed. For instructions on upgrading a current installation, see *Upgrading NetProwler* on page 2.13.

To install NetProwler:

1. Log into the system as administrator, or administrator equivalent.
2. Insert the CD-ROM in the drive.
3. Exit any programs that may be running.

   At the end of the installation process, NetProwler restarts the system.
4. Select **Run** from the Windows **Start** menu, click **Browse,** and then select the CD-ROM drive.
5. Select **NetProwlerSetup.exe,** and then click **OK**.

   The Welcome dialog box appears.

Welcome to NetProwler Installation
Welcome!
This program will install NetProwler on your computer. Press Cancel to abort the Install! Please ensure that all programs / services using ODBC are stopped.
OK
Cancel

Figure 2-4: NetProwler Welcome Screen

6. Close all applications and stop all Open Database Connectivity (ODBC) utilities, and then click **OK**.

   If NetProwler detects that your system has more than one NIC card, it displays the Adapter List dialog box. If your system has only one NIC card, the Adapter List dialog box does not appear.

   AXENT recommends that you install NetProwler on a system with only one NIC card.

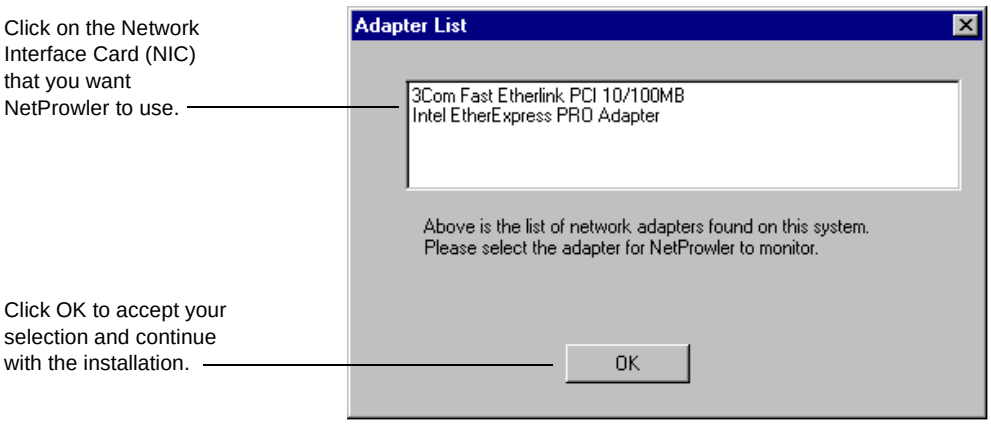

Click on the Network Interface Card (NIC) that you want NetProwler to use.
Adapter List
3Com Fast Etherlink PCI 10/100MB
Intel EtherExpress PRO Adapter
Above is the list of network adapters found on this system.
Please select the adapter for NetProwler to monitor.
Click OK to accept your selection and continue with the installation.
OK

Figure 2-5: Adaptor List Dialog Box

7. Click on the adapter that you want NetProwler to use to monitor the network segment, and then click **OK**.

   The NetProwler License dialog box appears.

8. Read the NetProwler license agreement, and then click **OK**.

The Select Destination Directory dialog box appears.

Figure 2-6: Select Destination Directory Dialog Box

9. To accept the default location and continue, click **OK.**

   Or

   Select the desired installation and location, and then click **OK**.

   The Setup program installs the files. After installing the files, the Add License dialog box appears

10. In the **License Key** field, type the 19-character license key.

    The license key and serial number are received from AXENT. If you do not have these numbers, please contact your AXENT account manager or e-mail AXENT's licensing administrator at *license@axent.com* to obtain them.

11. Click **OK**.

    NetProwlerSetup places the NetProwler icon in the Start-up menu so that NetProwler automatically starts when you start the system. The NetProwler dialog box appears. This box contains information about your installation and how to contact AXENT.

12. Click **OK**.

    The Install dialog box appears. The system must be restarted.

13. Click **OK**.

    NetProwler is installed.

Uninstalling NetProwler

To uninstall NetProwler:

1. From the **Start** menu, select **Programs**, **NetProwler**, and then **Uninstall**.

   The Uninstalling the NetProwler Application dialog box appears.

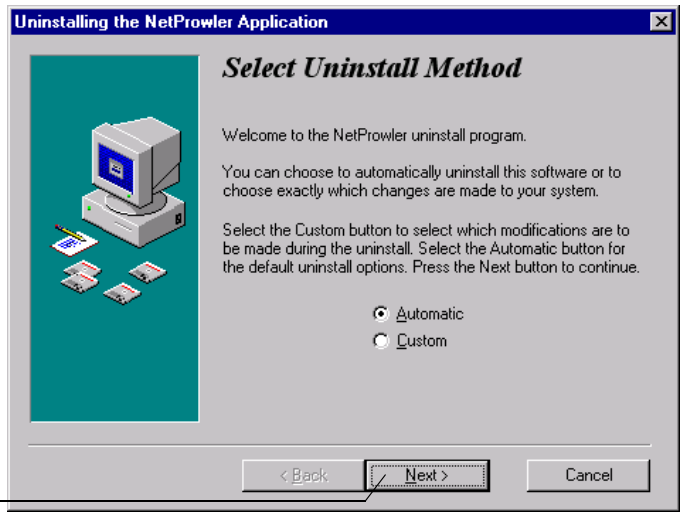

Uninstalling the NetProwler Application
Select Uninstall Method
Welcome to the NetProwler uninstall program.
You can choose to automatically uninstall this software or to choose exactly which changes are made to your system.
Select the Custom button to select which modifications are to be made during the uninstall. Select the Automatic button for the default uninstall options. Press the Next button to continue.
Automatic
Custom
< Back
Next >
Cancel
Click Next.

Figure 2-7: Uninstalling the NetProwler Application Dialog Box

2. To automatically uninstall NetProwler, select **Automatic**, and then click **Next**. (Skip to **Step 9**.)

   Or

To choose which modifications are made to your system, select **Custom**, and then click **Next**. (Continue with **Step 3**.)

3. In the **Select Private Files to Remove** box, select the files to remove, and then click **Next**.
4. In the **Select System Files to Remove** box, select the files to remove, and then click **Next**.
5. In the **Select Directories to Remove** box, select the desired directories, and then click **Next**.
6. In the **Select Registry Keys to Remove** box, select the desired Registry Keys, and then click **Next**.
7. In the **Select Registry Keys to Edit** box, select the desired Registry keys, and then click **Next**.
8. In the **Select Sub-systems to Remove** box, select the desired subsystems, and then click **Next**.
9. In the **Perform Uninstall** box, click **Finish**.

   The uninstallation program removes the selected files.

Upgrading NetProwler

NetProwler is easily upgradable. The NetProwlerSetup program automatically detects when a system has an older version of NetProwler installed. You can choose to keep your current configuration or delete your current configuration and start fresh. If you keep your current configuration, NetProwler retains any generated reports, all of the entries in the Address Book, and common, custom, and predefined attack signature configurations for all systems in the address book.

To upgrade NetProwler:

1. Log into the system with administrative privileges.
2. Insert the NetProwler 3.0 CD-ROM in the CD-ROM drive.
3. Exit any programs that may be running.

   At the end of the installation process, NetProwler restarts the system.
4. Select **Run** from the Windows **Start** menu, click **Browse**, and then select the CD-ROM drive.
5. On the CD-ROM, select **NetProwlerSetup.exe** and click **OK**.

The Welcome dialog box appears.

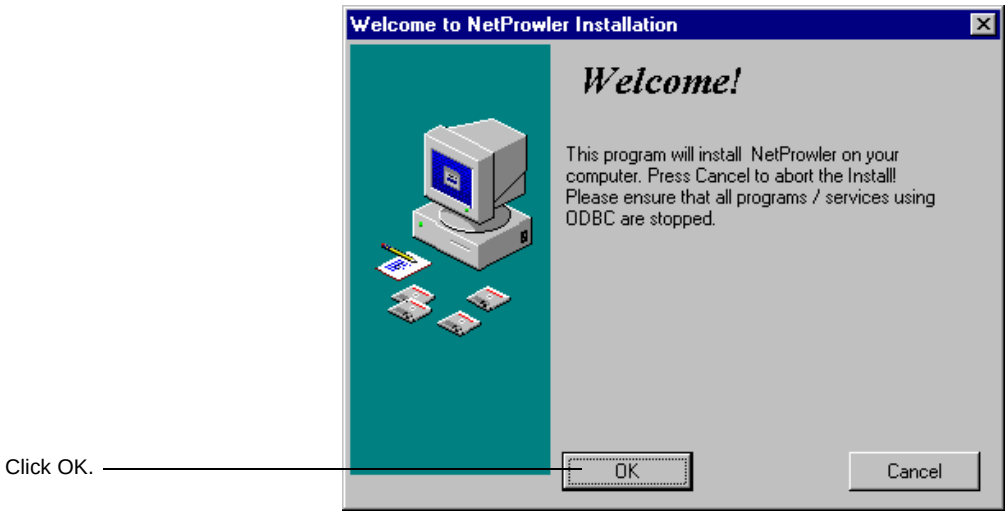

Welcome to NetProwler Installation
Welcome!
This program will install NetProwler on your computer. Press Cancel to abort the Install!
Please ensure that all programs / services using ODBC are stopped.
OK
Cancel
Click OK.

Figure 2-8: NetProwler Welcome Screen

6. Stop any program or services that are using Open Database Connectivity (ODBC), and then click **OK**.

   The NetProwler License dialog box appears.

7. Read the NetProwler license agreement, and then click **OK**.

The NetProwler Install Found dialog box appears. This dialog box only appears when the NetProwler installation program discovers a previous installation on the system.

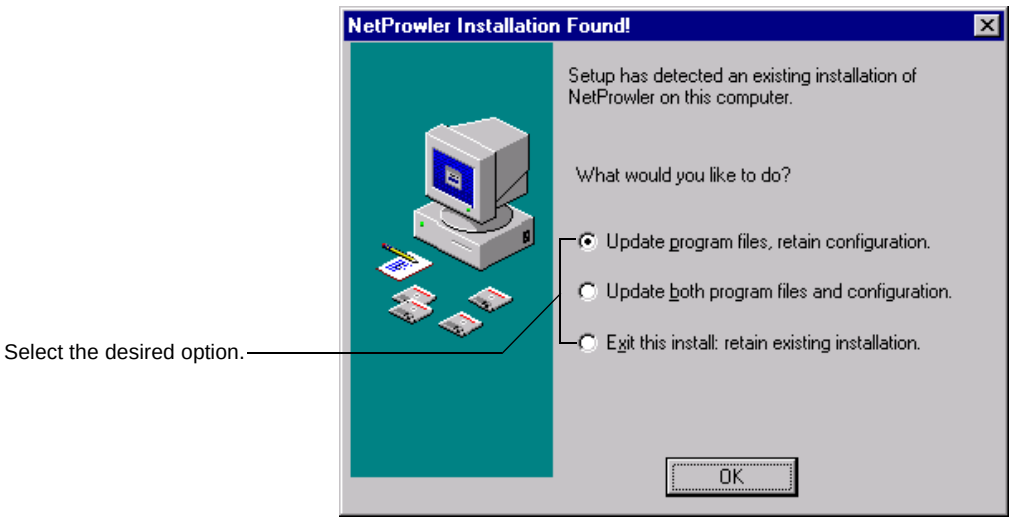

NetProwler Installation Found!
Setup has detected an existing installation of NetProwler on this computer.
What would you like to do?
Update program files, retain configuration.
Update both program files and configuration.
Exit this install: retain existing installation.
OK
Select the desired option.

Figure 2-9: NetProwler Install Found Dialog box

To upgrade the software and retain your existing configuration, select the **Update program files, retain configuration** radio button, and then click **OK**. (Recommended)

Or

To upgrade the software and remove the existing configuration, select the **Update both program files and configuration** radio button, and then click **OK**.

Or

To exit, select the **Exit this install: retain existing installation** radio button, and then click **OK**.

8. In the **Add Licenses** dialog box, type the 19-character **License Key** and **Serial Number**, and then click **OK**.

   The Setup program installs the NetProwler software. After installing the software, the Successful Installation screen appears.

9. Click **OK**.

   The NetProwler information dialog box appears. This box describes information about the installation and how to contact AXENT.

10. Click **OK**.

    The Install dialog box appears. The system must be restarted.

11. Click **OK**.

    The system will restart. The new version of NetProwler is installed.

Chapter 3

Touring NetProwler

Overview

NetProwler monitors TCP/IP traffic on a network segment to detect and respond to network-based intrusion attacks. NetProwler's graphical user interface, the NetProwler Console, controls all of NetProwler's features. This chapter introduces the different elements of the NetProwler Console and explains how to use the console to configure NetProwler and view the intrusion attacks that NetProwler detects. Chapter topics include:

- Starting the NetProwler Console
- The NetProwler Console
- The Menu bar
- The Toolbar
- The Configure tree and pane
- The Monitor tree and pane
- Stopping NetProwler

Starting the NetProwler Tour

This tour introduces you to the NetProwler Console and its components. It begins by explaining how to start NetProwler. After starting NetProwler, the tour provides an overview of the Console screen and introduces you to the Menu and Toolbar. It explains the NetProwler features that you can access from these Console components.

Next, the tour introduces you to the Configure window which is divided into the Configure tree and pane. The tour explains the different branches in the Configure tree and the features that you can configure in the corresponding lists in the Configure pane.

After configuring NetProwler in the Configure window, you can view NetProwler's results in the Monitor window. The tour explains the Monitor tree and pane and illustrates the types of information that you might see in the pane.

Finally, the tour describes how to stop NetProwler.

Starting the NetProwler Console

To start NetProwler:

1. From the Windows **Start** menu, choose **Programs**, **Axent**, and then **NetProwler.**

The NetProwler Authentication dialog box appears.

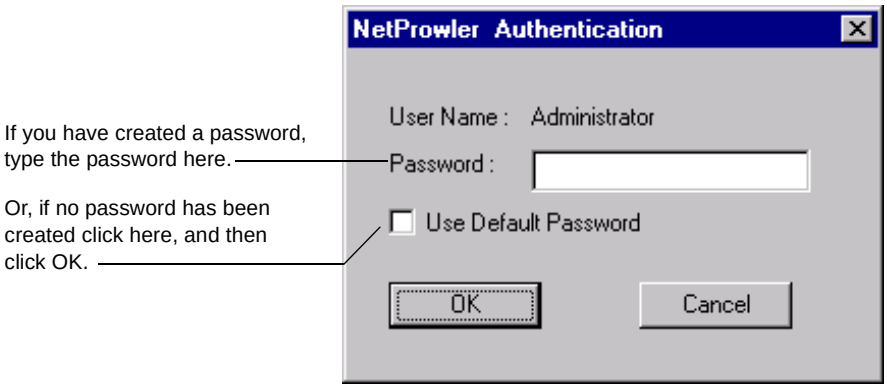

If you have created a password, type the password here.
Or, if no password has been created click here, and then click OK.
NetProwler Authentication
User Name : Administrator
Password :
Use Default Password
OK
Cancel

Figure 3-1: NetProwler Authentication Dialog Box

2. If an administrative password has been created, click in the **Password** box, type the administrative password, and then click **OK**.

   Or

   If no password is configured, click the **Use Default Password** check box, and then click **OK**.

   The Authentication dialog box appears. AXENT recommends creating an administrative password so that only authorized administrators can modify NetProwler's configuration and view network-based intrusions.

3. Click **Change** to create NetProwler's new administrative password.

   Or

   Click **Continue** to start the NetProwler Console.

If the administrative password is forgotten, NetProwler must be re-installed and a new administrative password created. There is no way to recover the old administrative password.

The NetProwler Console is started and the system's Network Interface Card is put in promiscuous mode. In promiscuous mode, NetProwler can process all the TCP/IP packets it sees. Once NetProwler is started, you can close the Console window, and NetProwler will continue to monitor the network. However, you will have to re-authenticate to open the Console window again.

The NetProwler Console

The NetProwler Console is a graphical user interface (GUI) used to configure and administer NetProwler. All of NetProwler's features are controlled in the NetProwler Console. The NetProwler Console contains the following elements:

- Menu bar
- Toolbar
- Configure tree and pane
- Monitor tree and pane

The following graphic illustrates the NetProwler Console screen elements. Please familiarize yourself with these elements.

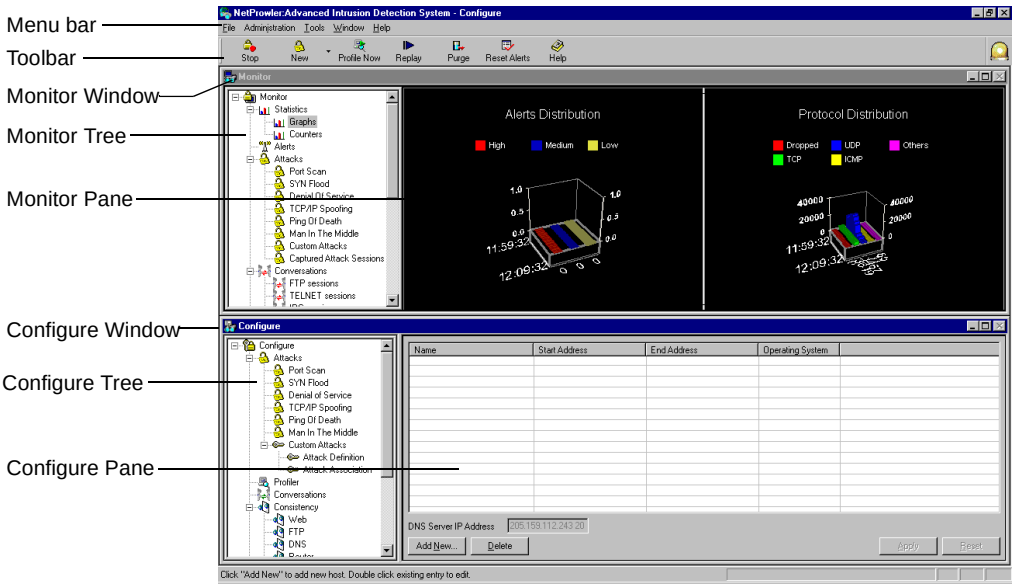


Figure 3-2: NetProwler Console Elements

The Configure window contains the Configure tree and pane. In the Configure tree, you select the feature that you want to configure. Then in the Configure pane, you set and apply your configuration options. The Configure pane displays the current settings for the objects selected in the Configure tree.

The Monitor window contains the Monitor tree and pane. The Monitor pane displays information about the objects that you select in the Monitor tree. Once you have configured NetProwler in the Configure tree, you can view the information about detected attacks and live network sessions on the monitored systems in the Monitor pane.

You can minimize the NetProwler Console and each of its windows. The Monitor window can be minimized and maximized without the need to re-authenticate. However, when you minimize either the NetProwler Console or the Configure window of the Console, you need to re-authenticate to reopen it. This prevents anyone from changing NetProwler's configuration

settings when you are away from the system. AXENT recommends that you minimize the Console or the Configure window if you are going to be away from the system.

Menu Bar

The Menu bar provides access to many of NetProwler's features. It contains the following menus:

- File
- Administration
- Tools
- Window
- Help

File Menu

The **File** menu contains the following items:

- **Stop Monitoring**—stops NetProwler from monitoring hosts
- **Replay Session**—replays a captured network session
- **Exit—**quits NetProwler

Administration Menu

The **Administration** menu contains the following items:

- **Sync New Signatures—**Synchronizes the latest pre-defined and/or user-defined attack signatures
- **Update License—**Updates the NetProwler license key
- **Purge Database**—Purges the Alerts database
- **Change Password**—Changes the NetProwler password

Tools Menu

The Tools menu contains the following items:

- **Profile Now**—Opens the Profiler configuration dialog
- **ASD Wizard**—Starts the Attack Signature Definition Wizard
- **Options**—Opens the NetProwler memory buffer configuration dialog

Windows Menu

The Windows menu contains the following items:

- **Cascade**—Arranges windows so they overlap
- **Tile**—Arranges windows as non-overlapping tiles
- **Configure**—Activates the Configure Window
- **Monitor**—Activates the Monitor Window

Help Menu

The Help menu contains the following items:

- **Contents**—Displays the NetProwler help file
- **About NetProwler**—Displays NetProwler program and version information

The Toolbar

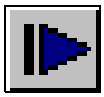
The toolbar provides quick access to the most common features of NetProwler.

The following list provides the name and function of each button.

Start/Stop Monitoring. Starts or stops NetProwler from monitoring the network.

Add New. Displays the correct dialog box to add a new attack signature definition, address book entry, application book entry, or access entry.

Profile Now. Starts the Profiler configuration dialog. The Profiler provides the most efficient method of adding and configuring network systems in NetProwler.



Replay. Allows you to replay a captured session.

Purge. Allows you to purge entries older than a specified date from the Alarm database.

Reset Alerts. Allows you to reset the alerts that the monitor pane displays.

Online Help. Access Online Help. In Online Help, you can browse or search by keywords.

The Configure Tree and Pane

The Configure Window contains the Configure tree and pane. In the Configure tree you can select the NetProwler feature that you want to configure. The Configure tree consists of eight major branches:

- Attacks
- Profiler
- Conversations
- Consistency
- Access
- Reports
- Address Book
- Notification Options

Once you select the feature in the Configure tree, you can create, view, or edit configuration settings for that feature in the Configure pane. The following graphic illustrates the Configure tree.

Select the NetProwler feature that you want to configure in the Configure tree.

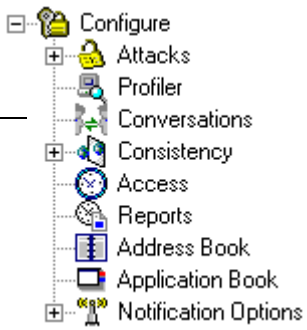


Figure 3-3: Configure Tree Branches and Objects

The following sections describe each branch in the Configure tree.

Attack Branch

In the Attack branch, you can associate Common, custom, and user-defined attack signatures with the network hosts that you want to monitor for those attacks. In addition, you can configure response attacks, specify authorized hosts or ports, and specify applications for custom and user-defined attacks. NetProwler groups attack signatures into three categories:

- **Common Attacks.** Common attacks signatures detect attacks that are frequently used and operating system independent.
- **Custom Attacks.** Custom attack signatures detect attacks targeted toward specific operating systems or applications. NetProwler comes with a number of pre-defined custom attack signatures ready for activation.
- **User-defined Attacks.** User-defined attacks are attacks that you create using NetProwler's Attack Signature Definition Toolkit.

The following graphic illustrates where the Common, custom, and user-defined attack signatures reside in the Attack branch. User-defined attack signatures are listed in the Custom Attacks branch with the pre-defined attack signatures

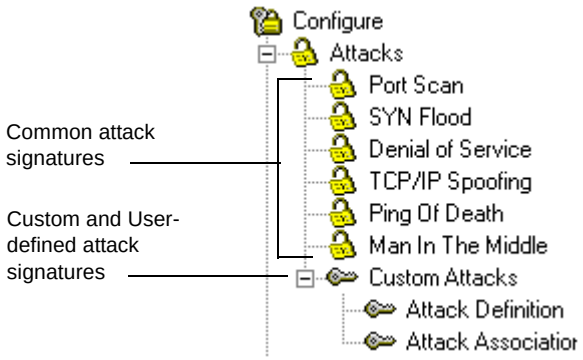


Figure 3-4: Attack Branch Objects

Click any of the Common attacks in the Attack branch and the Configure pane displays an association list for that attack. The list includes each host that has been added to the NetProwler

Address Book. You can enable or disable the attack signature for each host by clicking the Selected column. A check mark indicates that the attack signature is enabled for the host. The following graphic illustrates the Port Scan Association list.

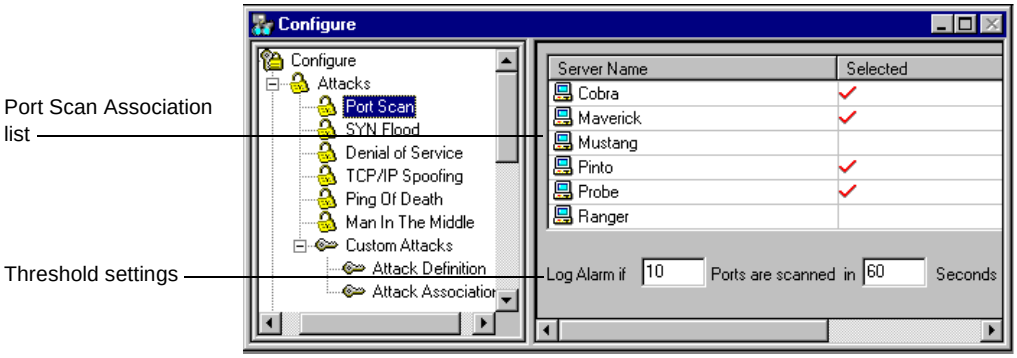


Figure 3-5: Port Scan List in the Configure Pane

Custom Attacks

Under the Custom Attacks branch, click the Attack Definition object, and the Configure pane displays a list of the custom attack signatures plus any user-defined attack signatures that you have created. This list provides a short description and other pertinent information about each attack signature. The following graphic displays a portion of the list of Custom attack signatures.

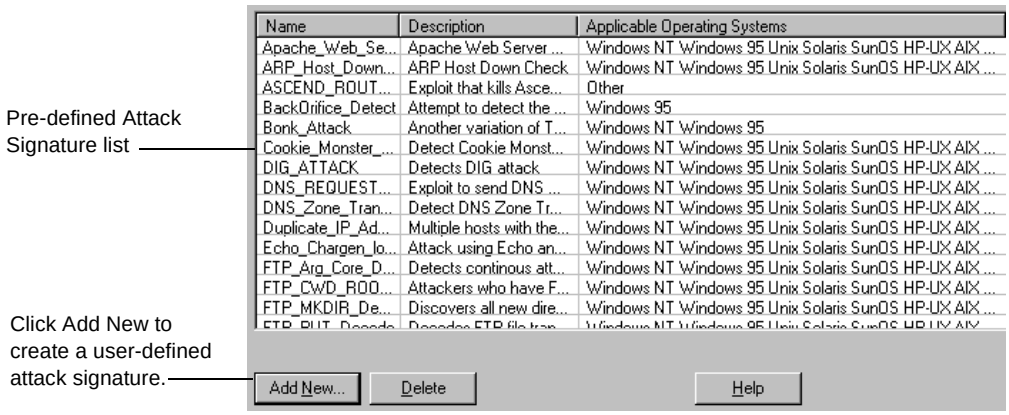

Pre-defined Attack Signature list
Click Add New to create a user-defined attack signature.
Name
Description
Applicable Operating Systems
Apache_Web_Se...
Apache Web Server ...
Windows NT Windows 95 Unix Solaris SunOS HP-UX AIX ...
ARP_Host_Down...
ARP Host Down Check
Windows NT Windows 95 Unix Solaris SunOS HP-UX AIX ...
ASCEND_ROUT...
Exploit that kills Asce...
Other
BackOrifice_Detect
Attempt to detect the ...
Windows 95
Bonk_Attack
Another variation of T...
Windows NT Windows 95
Cookie_Monster_...
Detect Cookie Monst...
Windows NT Windows 95 Unix Solaris SunOS HP-UX AIX ...
DIG_ATTACK
Detects DIG attack
Windows NT Windows 95 Unix Solaris SunOS HP-UX AIX ...
DNS_REQUEST...
Exploit to send DNS ...
Windows NT Windows 95 Unix Solaris SunOS HP-UX AIX ...
DNS_Zone_Tran...
Detect DNS Zone Tr...
Windows NT Windows 95 Unix Solaris SunOS HP-UX AIX ...
Duplicate_IP_Ad...
Multiple hosts with the...
Windows NT Windows 95 Unix Solaris SunOS HP-UX AIX ...
Echo_Chargen_lo...
Attack using Echo an...
Windows NT Windows 95 Unix Solaris SunOS HP-UX AIX ...
FTP_Arg_Core_D...
Detects continous att...
Windows NT Windows 95 Unix Solaris SunOS HP-UX AIX ...
FTP_CWD_ROO...
Attackers who have F...
Windows NT Windows 95 Unix Solaris SunOS HP-UX AIX ...
FTP_MKDIR_De...
Discovers all new dire...
Windows NT Windows 95 Unix Solaris SunOS HP-UX AIX ...
Add New...
Delete
Help

Figure 3-6: Pre-defined Attack Definition list

Attack Signature Definition Toolkit

Unlike any network-based intrusion detection tool on the market today, NetProwler provides an Attack Signature Definition (ASD) toolkit. This feature lets you create your own attack signatures and dynamically activate them in NetProwler.

Click Add New in the Pre-defined Attack Signatures list to access the ASD tool. The following graphic illustrates the Attack Signature Definition dialog box where you create a user-defined attack signature.

NetProwler's Attack Signature definition (ASD) tool (General Tab)

Use this tab to define the attack signature and how it is used.

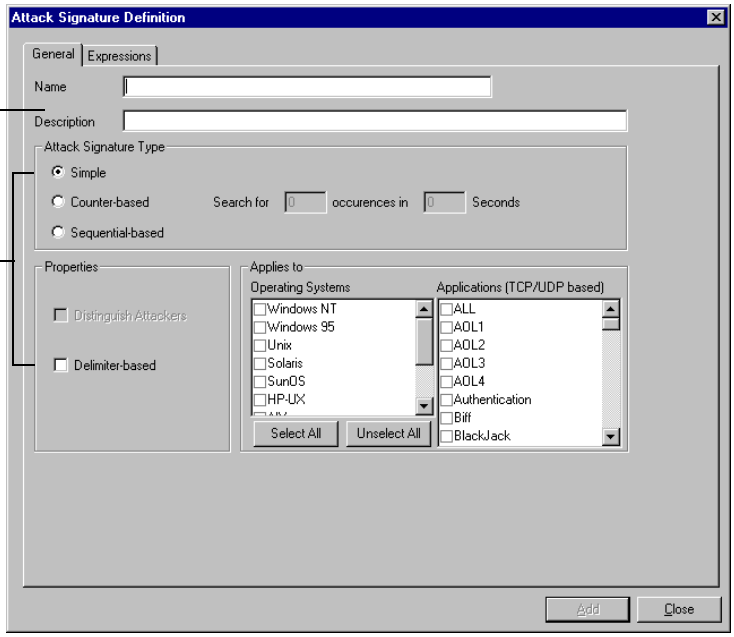


Figure 3-7: Attack Signature Definition Dialog Box

The Expressions tab in the Attack Signature Definition dialog box lets you define the attack signature's search criteria.

The Following graphic illustrates the Expressions tab.

NetProwler's Attack Signature Definition (ASD) toolkit (Expressions tab)

Use this tab to define the attack signature's search criteria.

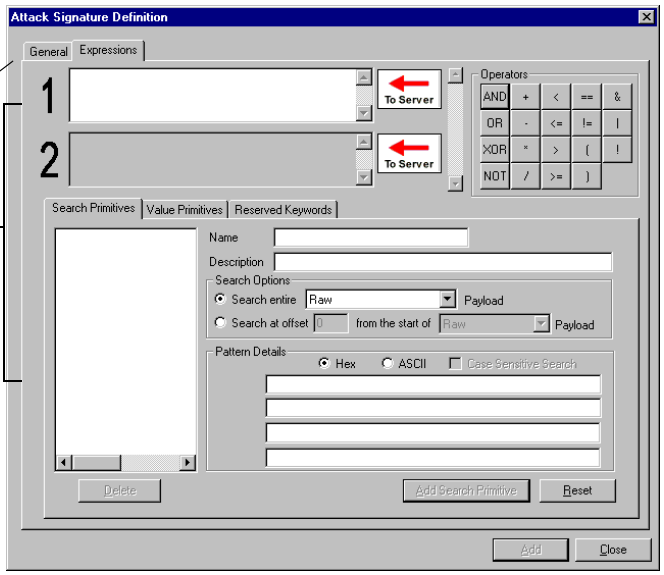


Figure 3-8: Attack Signature Dialog Box -Expressions Tab

Under the Custom Attacks branch, click the Attack Association object, and the Configure pane displays the Custom Attacks Association list. This list includes each host or range of hosts that have been added to the NetProwler Address Book, the host's operating system, and the number of custom attack signatures that are associated with the host.

Custom Attacks Association list

Host Name	Operating System	Number of Attacks Active
Cobra	Windows NT	90
Maverick	Windows NT	90
Mustang	Windows NT	90
Pinto	Windows NT	90
Probe	Windows NT	90
Ranger	Windows NT	90

Figure 3-9: Custom Attack Association List

In the Configure Pane, double-click a host name to open the Edit Attack Associations dialog box. In this dialog box, you can associate attack signatures with a monitored host or a range of hosts and set an attack signature's priority level. The following graphic illustrates the Edit Attack Associations dialog box.

Associated an attack signature with a host by moving the attack signature from the Available Attacks list to the Applied Attacks list.

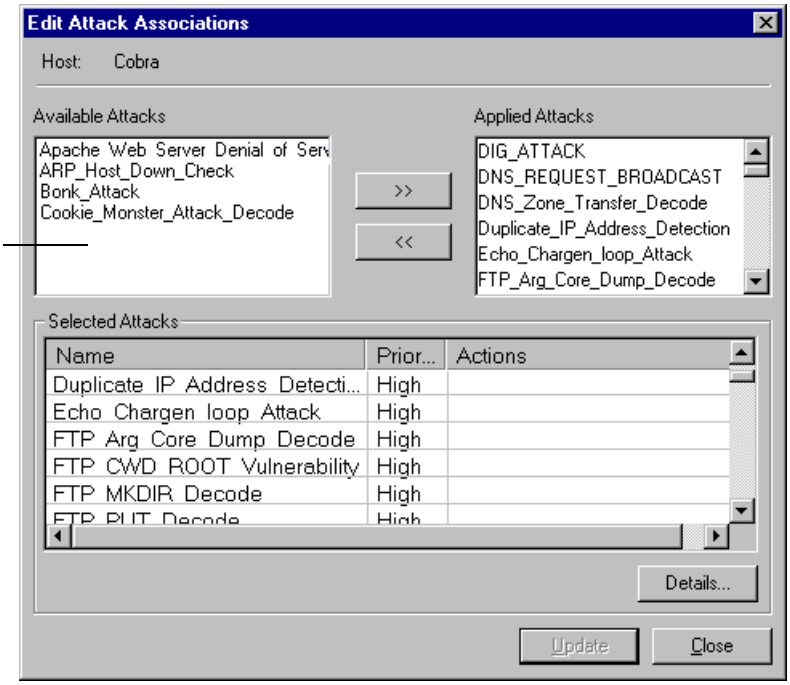


Figure 3-10: Edit Attack Associations Dialog Box

Under the Selected Attack box, select an attack, and then click Details to open the Edit Attack Association Details dialog box. The following graphic illustrates the Edit Attack Association Details dialog box.

Click a check box to associate a Response action to a an attack signature.

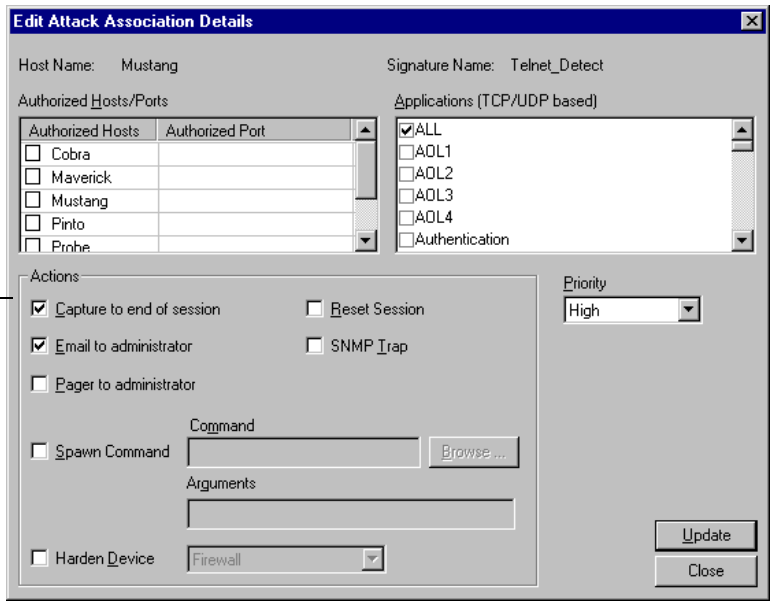


Figure 3-11: Edit Attack Association Details dialog box

In this dialog box, you can perform the following operations:

- Allow exclusions to NetProwler's attack reporting, (i.e., authorized hosts)
- Modify the TCP/UDP applications to which the attack applies
- Select response actions
- Change an attack signature's priority level

Profiler Branch

NetProwler protects against network-based intrusion attacks by monitoring configured hosts in a network segment. Each host that you want NetProwler to monitor must be listed and configured in the NetProwler Address Book.

The easiest and most efficient way to add systems to the Address Book is NetProwler's configuration tool, the Profiler.

The Profiler scans the network for "live" systems and devices. When it discovers a live system, the Profiler scans the system to identify what services are available on that system. The Profiler identifies the system, adds that system to the list of potential systems to monitor, and automatically suggests a list of attack signatures to associate.

You can also start the Profiler by clicking the Profile Now button on the Toolbar. The Start Scan dialog box appears as shown in the following graphic.

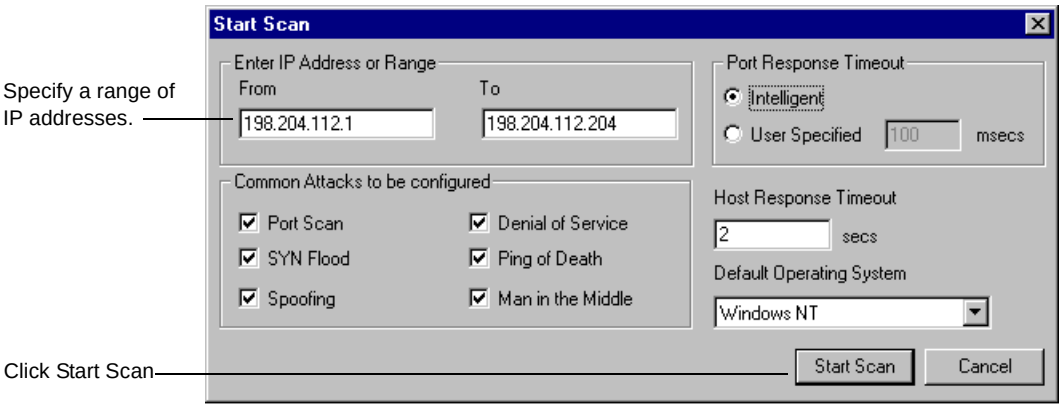


Figure 3-12: Start Scan Dialog Box

Enter the range of IP addresses to scan and click the Start Scan button. Once you have started the Profiler, you can click the Profiler branch in the Configure tree to display the Profiler Results screen. As illustrated in the following graphic, the Profiler Results screen lists the host name, IP address, and operating system of the network systems that the Profiler

discovered. It also lists how many attack signatures are applied to a specific host and whether or not attack signature configuration is enabled for that system.

The Profiler Results screen displays the network systems and devices that the Profiler's scan discovers.

Click the Change button to open the Profiler Schedule dialog box.

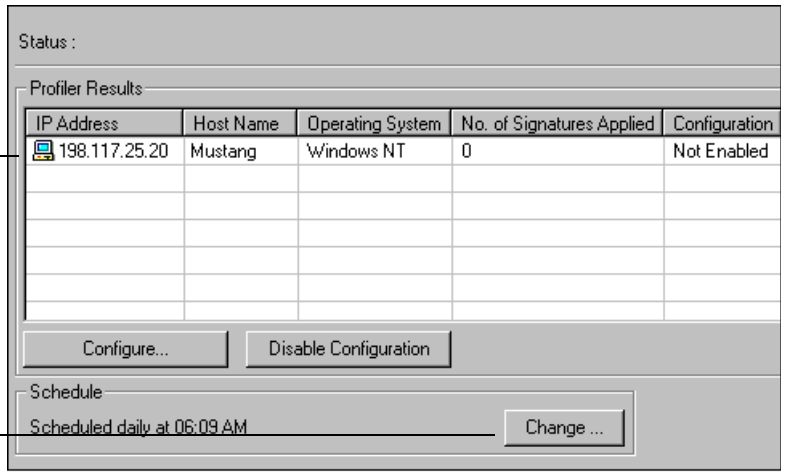


Figure 3-13: Profiler Results Screen

By selecting an entry and clicking Configure, you can open the Edit Attack Associations dialog box. In this dialog box, you can apply attack signatures to a host, configure options such as attack priorities or response actions, and add the entry to the Address Book.

The Profiler retains the network systems and devices that it discovers in the Profiler Results screen until you re-run the Profiler or until NetProwler is turned off. As long as the system still remains in the Profiler Results screen, you can disable its attack signature configuration in the Profiler Results screen. This removes the system from the Address Book as well.

Once an entry is removed from the Profiler Results screen, you must edit its attack associations in the Edit Attack Associations dialog box. You can open the Edit Attack Associations dialog box by selecting the Attack Associations branch, right-clicking the system, and clicking Modify.

For more information on configuring the Profiler, see *Chapter 4: Building the Address Book*

Scheduling the Profiler

The Profiler scheduling tool rescans the network and automatically associates attack signatures with new hosts based on the type of operating system and available services.

Network configurations change frequently as computers and other network devices get reconfigured, relocated, or removed from the network. NetProwler's Profiler Scheduling tool makes it easier to keep network security current by reprofiling the network at regular intervals. Reprofiling the network tells you which systems are now "live" or have been added since the last scan.

To ensure that the Profiler detects the maximum number of "live" systems, you should schedule the Profiler to run during times when the systems are most likely to respond. For example, profiling the network during normal work hours is more likely to find live systems than profiling late at night.

You can schedule the Profiler by clicking the Profiler branch, and then clicking Change in the Profiler Results screen. The following graphic illustrates the Profiler Schedule dialog box.

The Profiler Scheduling feature makes it easier to keep network security current. You can reprofile the network at regular intervals to detect new "live" systems.

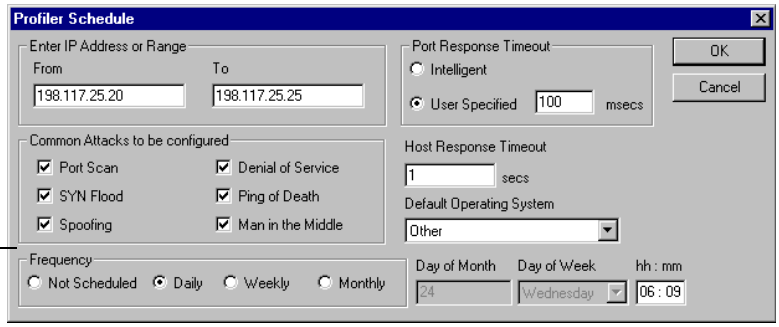


Figure 3-14: Profiler Schedule Dialog Box

Consistency Branch

NetProwler can check important resources on the network servers that it protects. For example, it can compare files on web and ftp servers on a byte-by-byte basis with files kept on

mirrored web and ftp servers. NetProwler can also check DNS hostname and router configuration files for corruption or tampering.

The following graphic illustrates the objects in the Consistency branch.

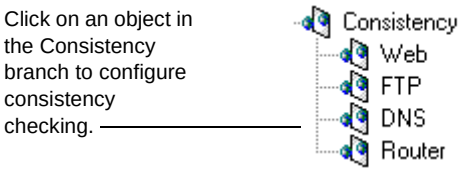


Figure 3-15: Consistency Branch

In the Consistency branch, click Web, FTP, DNS, or Router to view the Scheduled Consistency Checks list for that object. You can perform four operations from this list:

- Create a new consistency check
- Edit an existing consistency check
- Schedule or reschedule an existing consistency check
- Delete a consistency check

The following graphic illustrates the list of scheduled consistency checks for web servers. The lists for other consistency checks are similar.

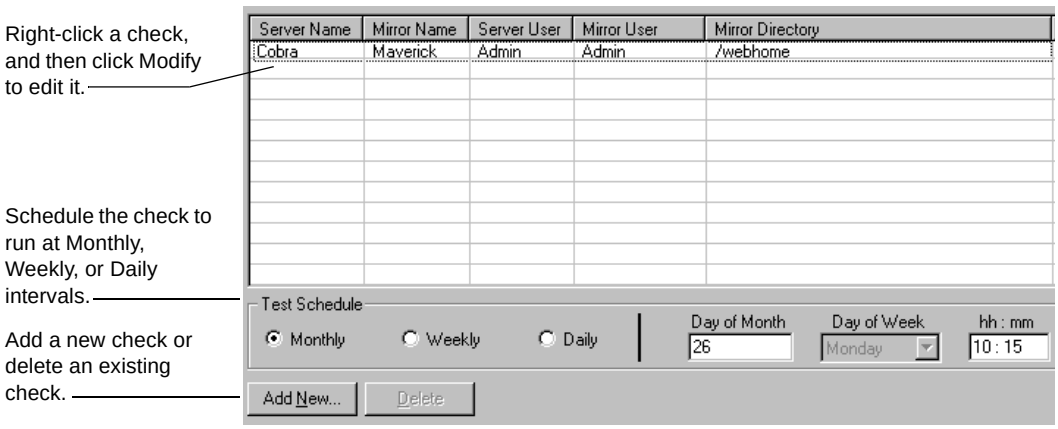


Figure 3-16: Consistency Check List

Conversations Branch

NetProwler can monitor TCP/IP session types, such as ftp, telnet, and HTTP, as they occur in real time. In the Conversations branch, you can check the types of TCP/IP sessions that you want to monitor on each designated system. You can also set NetProwler to purge a session from the monitor when the session has been inactive for a user-determined number of minutes.

A system must be listed in the Address Book before you can configure NetProwler to monitor it. You can enter systems to the Address Book either manually or via the Profiler. The following graphic illustrates the Conversations branch in the Configure Pane.

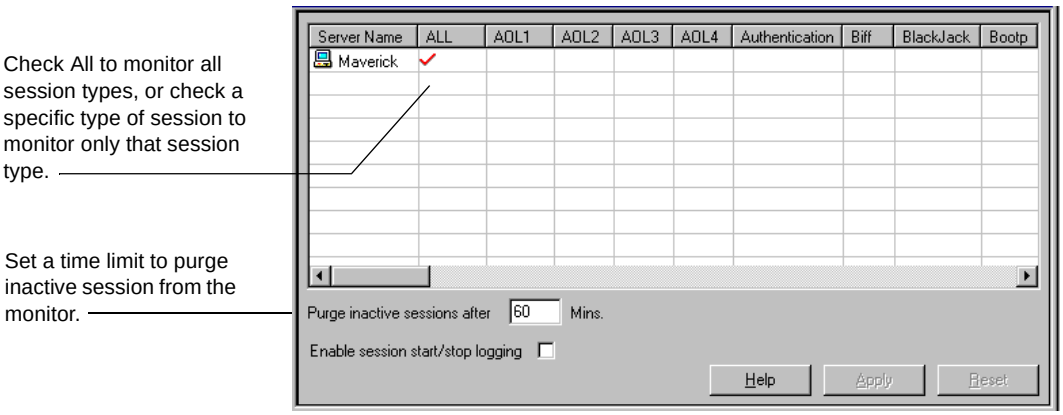


Figure 3-17: Conversation Branch

Access Branch

NetProwler can stop or limit all or specific types of TCP/IP-based communication without modifying client or server workstations. You can limit access at certain times of the day or days of the week. NetProwler generates an alert message whenever someone tries to access a service on a system that has access limits set for that service.

You can use the limit access feature when you want to give outside users access to a system only at specific times. For example, you could access telnet access to an important system only during normal hours.

Click the Access branch and the Configure pane displays the settings for the systems that you have set time access limits on. From this list, you can also create new time access limits and modify or delete existing limits. The following graphic illustrates the Access Time Limits list.

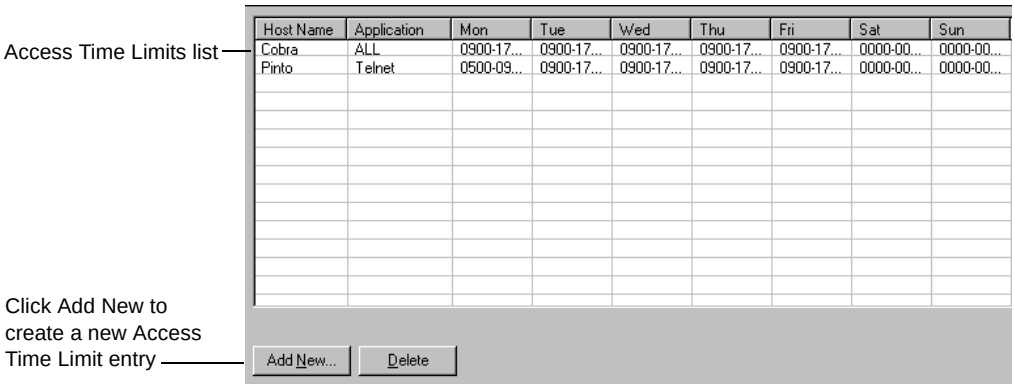


Figure 3-18: Access Branch

Reports Branch

The Reports branch displays the name, report type, frequency, and scheduled status of any reports that you have created and scheduled. From this list, you can perform the following tasks:

- Create new reports
- Schedule reports
- Modify scheduled reports
- Delete scheduled reports

The following graphic illustrates the Reports list in the Configure pane.

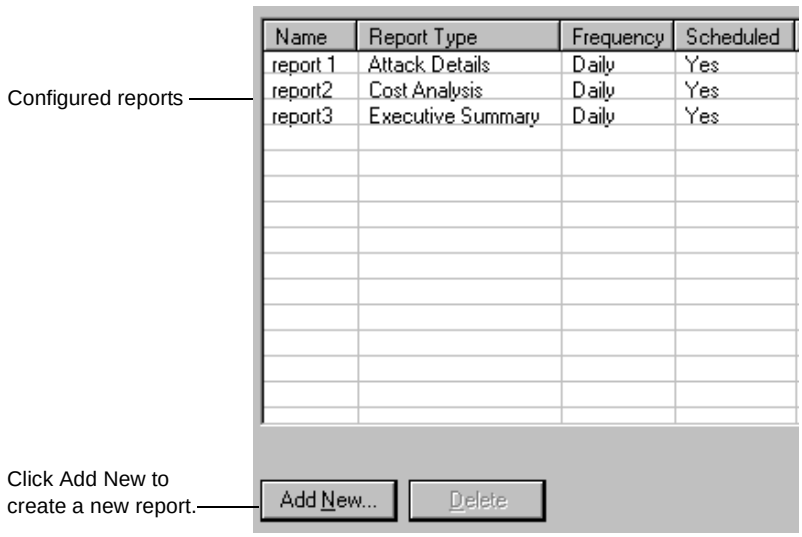


Figure 3-19: Reports List in the Configure Pane

NetProwler's report generation feature lets you generate three different types of reports:

- Attack Details
- Executive Summary
- Cost Analysis

Attack Details. The Attack Details report describes any attacks that have taken place during a specified reporting period. It shows the type of attacks, time of the attacks, the attacking system, and the attacked system.

Executive Summary. The Executive Summary report presents an overview of the number and risk level of attacks detected in a specified time period compared with the number of attacks expected at each risk level.

Cost Analysis. The Cost Analysis report takes figures that you provide and estimates how much the attacks detected during a given time period cost you.

Generated reports are displayed in the Generated Reports branch of the Monitor tree.

Address Book Branch

The Address Book branch lists the network systems and devices that NetProwler will monitor for intrusion attacks. NetProwler only monitors those systems and devices that you enter in the Address Book. Systems can be added via the Profiler or manually.

In the Address Book list, you can manually add new systems to monitor, delete systems from the Address Book, and edit a host's definition. The following graphic illustrates the Address Book list.

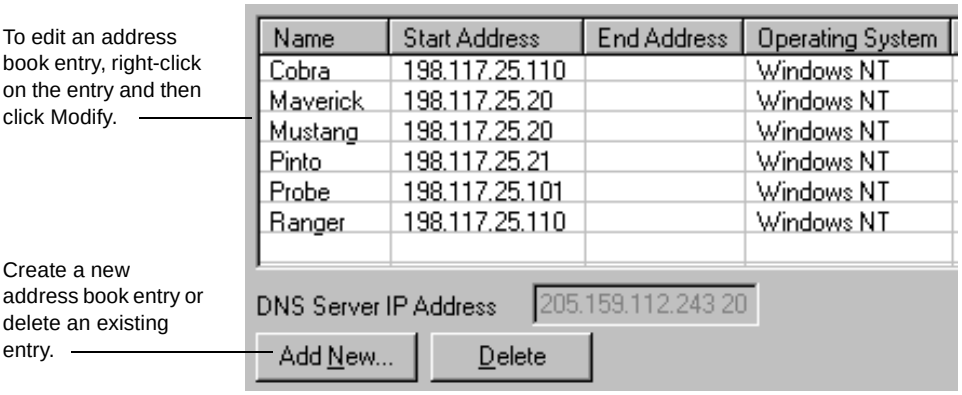

To edit an address book entry, right-click on the entry and then click Modify.
Create a new address book entry or delete an existing entry.
Name
Start Address
End Address
Operating System
Cobra 198.117.25.110 Windows NT
Maverick 198.117.25.20 Windows NT
Mustang 198.117.25.20 Windows NT
Pinto 198.117.25.21 Windows NT
Probe 198.117.25.101 Windows NT
Ranger 198.117.25.110 Windows NT
DNS Server IP Address
205.159.112.243 20
Add New...
Delete

Figure 3-20: NetProwler Address Book List

Application Book Branch

NetProwler comes configured with 70 application types in its Application Book. An application is a low-level or end-user program, such as ftp, telnet, or rLogin, that uses TCP or UDP protocols. NetProwler uses the list of configured applications to monitor network sessions and scan ports and services during profiling. It stores the list of applications in the Application Book.

Clicking on the Application Book in the Configure tree displays the list of configured applications.

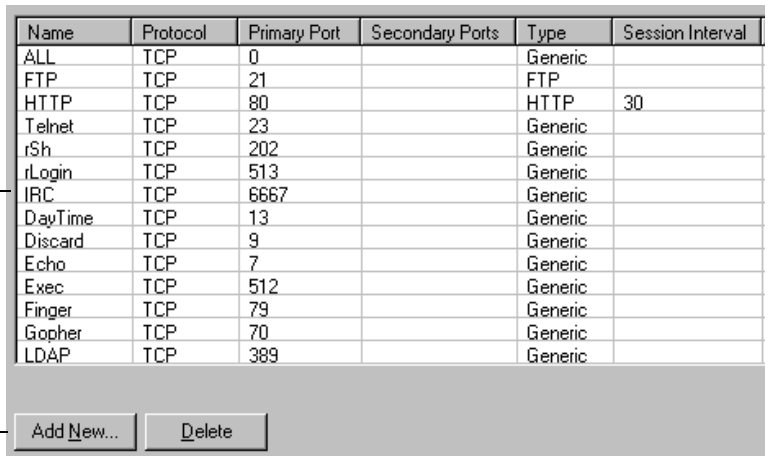


Figure 3-21: Application Book Branch

The Application book lists contains the following information about the application:

- Name
- Protocol
- Primary Port
- Secondary Port
- Type (FTP, HTTP / UDP, Generic)
- Session Interval

You can add new applications to the list and edit or delete existing applications.

Notification Options Branch

The Notification Options branch lets you set and review the notification actions that NetProwler takes when it detects an intrusion attack. You can set NetProwler to take the following notification actions:

- Page an administrator
- E-mail an administrator
- Notify a Raptor or Check Point FireWall-1® firewall (the firewall can be configured to respond to that notification by preventing the attacking source from entering the firewall for a period of time ranging from one minute to forever.)
- Send SNMP traps to SNMP Managers

The following graphic illustrates the objects in the Notification Options branch.

You can set and review NetProwler notification options in the Notification Options branch of the Configure tree.

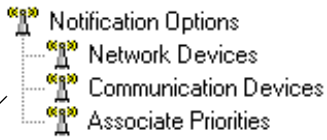


Figure 3-22: Notification Options Branch

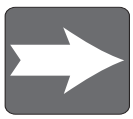
Network Devices

Click the Network Devices branch to display the firewall and SNMP notification options.

When you select the firewall notification option and associate it with a specific attack, NetProwler responds to the attack by sending a Suspicious Activity Monitoring Protocol (SAMP) message to the Firewall-1 firewall. The Firewall-1 firewall can then direct the firewall to terminate the sessions or deny access to the host generating the attack.

You will need to configure the desired firewall responses on the Firewall-1 firewall itself. You will also need to associate the notification option to a specific attack in the Edit Attack Associations dialog box. The Edit Attack Associations dialog box is accessible through the Attack Associations branch of the Configure tree.

Along with firewall hardening, you can configure your SNMP traps notification action from the Network Devices object screen. You can configure NetProwler to send SNMP traps to up to two SNMP Managers, which can be configured to act on the SNMP traps.



Intruder Alert can be configured to process SNMP traps. This allows you to take advantage of the powerful response mechanisms contained in Intruder Alert. To learn how to configure Intruder Alert to receive SNMP traps sent from NetProwler, please refer to the *NetProwler-Intruder Alert Integration Manual* that shipped with the NetProwler CD-ROM.

Communication Devices

When you click on the Communications object, the Configure pane displays the pager and e-mail notification options.

The pager notification option uses a configured modem to send the notification message to a paging service, which then pages the administrator. In the Pager Options group, you select the communication port on which the modem is configured and enter the phone number of the paging server with any required pager commands.

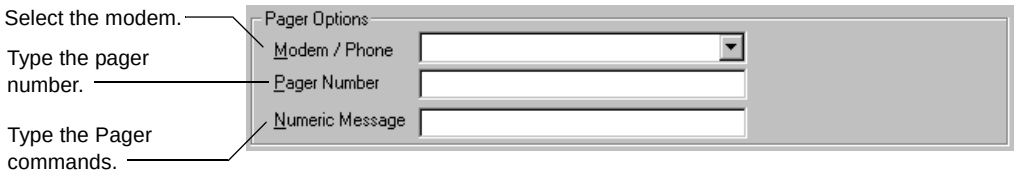


Figure 3-23: Pager Options - Communication Devices Branch

In the E-mail options group, you type the e-mail address and the mail server IP address.

Figure 3-24: E-mail Options - Communication Options Branch

Once you have configured NetProwler's pager and e-mail notification options, you need to associate them with an attack priority or a specific attack signature on a specific monitored host before NetProwler will perform the notification action.

Associate Priorities

When you click Associate Priorities, the Configure pane displays the notification options that you can set for each priority level: high, medium, or low. For example, the screen settings illustrated in the following graphic configure NetProwler to harden a firewall and send SNMP traps whenever it detects an attack signature with a high priority. But whenever it detects an attack signature with a medium or low priority, NetProwler sends an e-mail notification to an administrator.

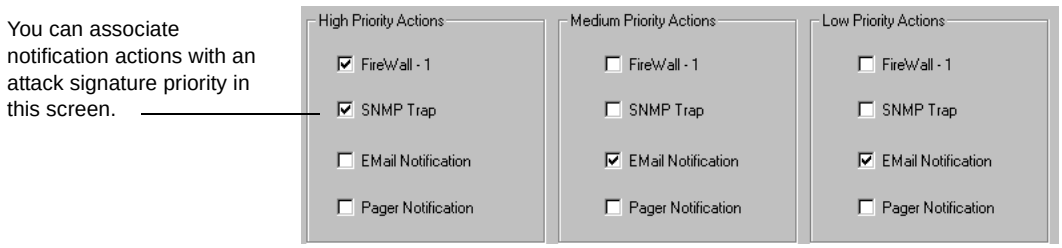


Figure 3-25: Associate Priorities Options

You can also set notification actions individually for each attack signature in the Edit Attack Associations dialog box. Notification options set in the Edit Attack Associations dialog box overrule those set in the Associate Priorities branch.

When NetProwler detects an attack it responds with the notification action or actions you configure for that attack's priority level.

The Monitor Tree and Pane

The Monitor Windows contains the Monitor tree and pane. The Monitor tree is organized in standard hierarchical structure. It contains seven major branches or tree objects:

- Statistics
- Alerts
- Attacks
- Conversations
- Consistency
- Access
- Reports

Selecting a branch or object in the tree displays information about the object in the Monitor pane. The following sections provide an example of the kinds of information that you might expect to see displayed for each branch of the Monitor tree.

Statistics Branch

The Statistic branch provides information on the alarms that NetProwler generated at each priority level. It also displays frame statistics such as the total number of frames processed and the number of frames dropped. It also lists the number of packets processed for each type of protocol. As the following graphic illustrates, the Statistics branch contains two objects: Graphs and Counters.

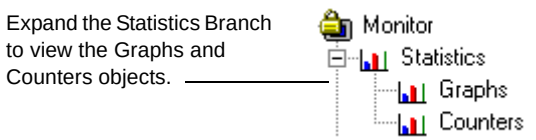


Figure 3-26: Statistics Branch in the Monitor Tree

Graphs. The Graphs object displays to the Alerts Distribution and Protocol Distribution graphs.

Alerts and Protocol Distribution Graphs

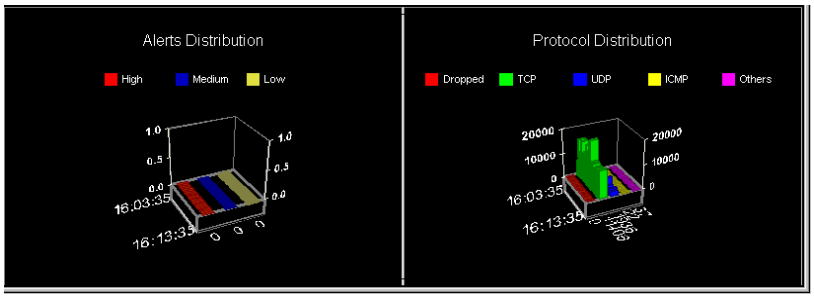


Figure 3-27: Alerts and Protocol Distribution Graphs

Counters. The Counters object, as shown in the following graphic, presents frame and protocol statistics.

Statistics indicate the number of frames processed and dropped.

Protocol Distribution displays the number of packets for each type of protocol.

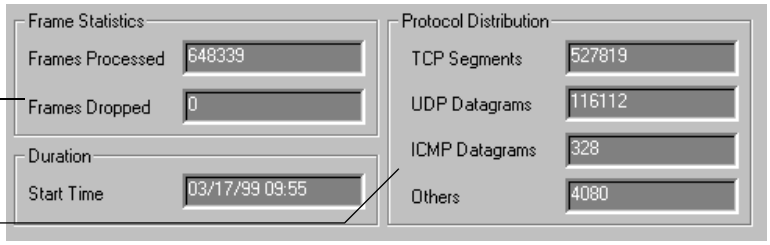


Figure 3-28: Frame Statistics Counter

Alerts Branch

When you select the Alerts branch, the Monitor pane displays the detected attacks. As illustrated in the following graphic, the Monitor pane displays the attacked host, service, attack type, attack time, and priority for each detected attack. For more details about the attack or network session, you can click on the Attacks or Conversations branch.

The Monitor pane displays the name and IP address of the attacked system. It also displays the type of attack, service, attack time, and priority of the attack.

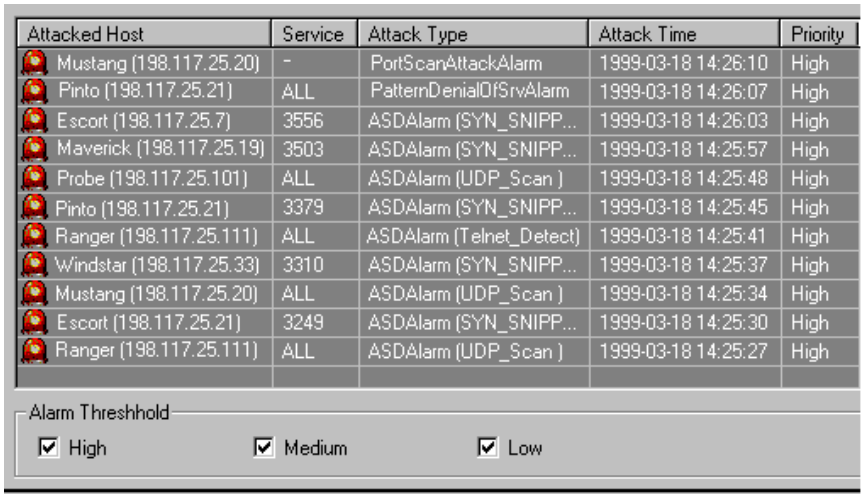

Attacked Host
Service
Attack Type
Attack Time
Priority
Mustang (198.117.25.20) - PortScanAttackAlarm 1999-03-18 14:26:10 High
Pinto (198.117.25.21) ALL PatternDenialOfSrvAlarm 1999-03-18 14:26:07 High
Escort (198.117.25.7) 3556 ASDAlarm (SYN_SNIPP... 1999-03-18 14:26:03 High
Maverick (198.117.25.19) 3503 ASDAlarm (SYN_SNIPP... 1999-03-18 14:25:57 High
Probe (198.117.25.101) ALL ASDAlarm (UDP_Scan) 1999-03-18 14:25:48 High
Pinto (198.117.25.21) 3379 ASDAlarm (SYN_SNIPP... 1999-03-18 14:25:45 High
Ranger (198.117.25.111) ALL ASDAlarm (Telnet_Detect) 1999-03-18 14:25:41 High
Windstar (198.117.25.33) 3310 ASDAlarm (SYN_SNIPP... 1999-03-18 14:25:37 High
Mustang (198.117.25.20) ALL ASDAlarm (UDP_Scan) 1999-03-18 14:25:34 High
Escort (198.117.25.21) 3249 ASDAlarm (SYN_SNIPP... 1999-03-18 14:25:30 High
Ranger (198.117.25.111) ALL ASDAlarm (UDP_Scan) 1999-03-18 14:25:27 High
Alarm Threshhold
High
Medium
Low

Figure 3-29: Alerts Branch

Attack Branch

The Attack branch provides more detailed information on the attacks than the Alert branch displays. The Attack branch contains objects for each of the six Common attacks, an object for all custom attacks, and an object for Captured Attack Sessions. Click an attack object in the Attack branch and the Monitor pane displays detailed information about detected instances of that type of attack. The Captured Attack Sessions lists captured sessions that you can replay.

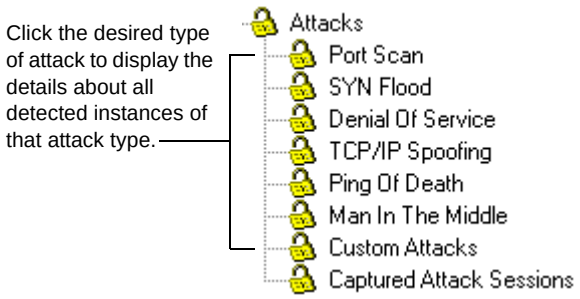

Click the desired type of attack to display the details about all detected instances of that attack type.
Attacks
Port Scan
SYN Flood
Denial Of Service
TCP/IP Spoofing
Ping Of Death
Man In The Middle
Custom Attacks
Captured Attack Sessions

Figure 3-30: Attacks Branch

Conversations Branch

The Conversations branch provides details about live network sessions. When the Monitor alerts you to a network session, for example a telnet detect message, you can expand the Conversations branch, click the session type, and view details on the session in the Monitor pane.

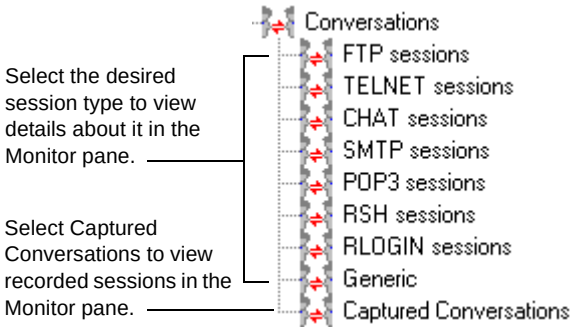


Figure 3-31: Conversations Branch

By clicking on the Details button, you can monitor the session as it occurs in real time. NetProwler even provides the option to terminate the session or record the session for later playback and analysis. The Captured Conversation object lists captured sessions that you can replay.

Consistency Branch

The Consistency branch provides information on NetProwler's consistency checks. NetProwler can perform consistency checking on web servers, ftp servers, DNS name servers, or router configuration files.

The Consistency branch provides information on NetProwler's consistency checks.

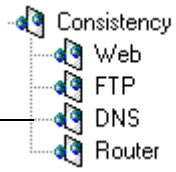


Figure 3-32: Consistency Branch

Clicking on an object in the Consistency branch displays information about the consistency checking for that object. For example, clicking on the Web object displays the name of the web server, the status of the check, and the results of the check.

The Monitor Pane displays the status of latest consistency check.

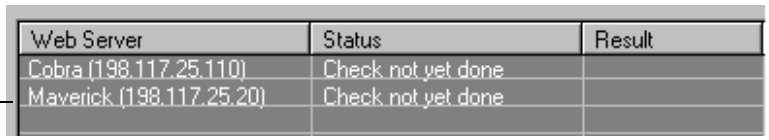


Figure 3-33: Web Server Consistency Check

Access Branch

The Access branch provides information on NetProwler's Time of Day Access feature. NetProwler can stop or limit traffic to TCP/IP based applications on one or more systems during certain times of the day and/or certain days of the week. Clicking the Access branch displays the following information in the Monitor pane:

- Each system on which you have set time access limits
- The applications that are limited

- The current status of the system (access allowed or access denied)
- The number of denied connection requests

The following graphic illustrates the Access branch.

The Access branch displays the current status of systems that have time access limits set.

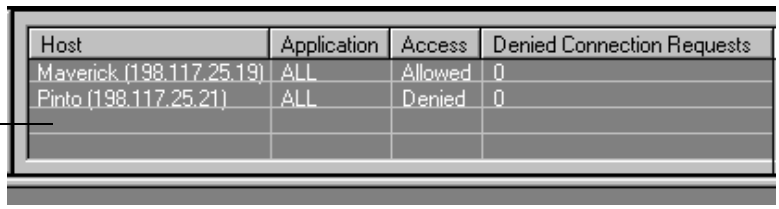


Figure 3-34: Access Branch -Time Access Limits

Reports Branch

The Reports branch provides information on NetProwler's generated reports and allows you to create queries on NetProwler alerts. As the following illustrates, the Reports branch contains two objects or sub-branches: Generated Reports and Query.

Expand the Reports branch to view the Generated Reports and Query objects.

Figure 3-35: Reports Branch

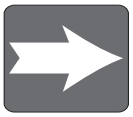
Generated Reports Branch

Click on Generated Reports branch in the Monitor tree and the Monitor pane displays the name of each generated report, the time that NetProwler generated the report, and the report's export type. You can double-click an entry to display the report.

To display a report, double-click the report in the Generated Reports list in the Monitor tree.

Report Name	Time generated	Export Type
report 119990322112323	1999-03-22 11:23:23	HTML
report219990322114624	1999-03-22 11:46:24	CSV

Figure 3-36: Generated Reports



TIP

A report does not show up in the Generated Reports list until after NetProwler has generated it. You can view scheduled reports in the Configure pane by clicking the Reports branch in the Configure tree.

Query Parameters

Click on Query Parameters in the Monitor tree and the Monitor pane displays query feature options. The Query feature lets you create a report that pinpoints particular types of information. For example, you can generate a query containing all of the high priority alerts that occurred over the weekend. You can save the query to a file for later viewing or distribution.

Clicking Query in the Monitor pane displays the Query feature options. You can use the Query feature to gather information about a particular aspect of network security.

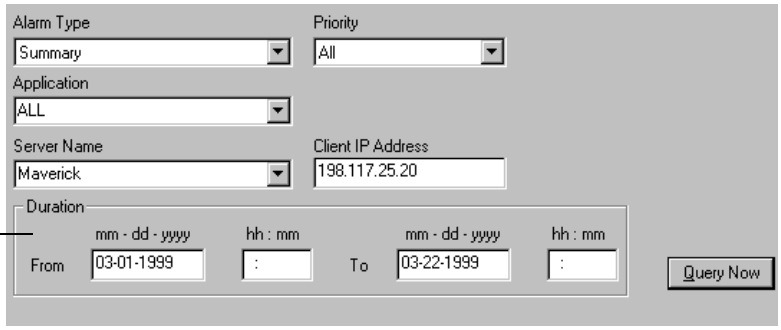


Figure 3-37: Query Parameters

Query Results

The Query Results pane displays the contents or results of the query. The results of the query can be saved in Comma Separated Value (CSV) format for later review or analysis in a third-party report generation program. If the result of the query does not contain the information you want, you can click the New Query button (in the lower right hand side of the Monitor pane) to modify the query parameters.

This completes the tour of the NetProwler Console. Thank you for taking time to learn more about this revolutionary information security product. The following section describes how to stop NetProwler.

Stopping NetProwler

Be aware that when the NetProwler Console is stopped, your network is left unprotected.

To keep your network protected, you should keep NetProwler on at all times.

To stop NetProwler:

1. From the **File** menu, choose **Exit**.

   Or

   On the Windows Taskbar Settings area, right-click the NetProwler icon, and then click **Exit**.

   The NetProwler Authentication dialog box appears. NetProwler only allows authorized users to shut it down.

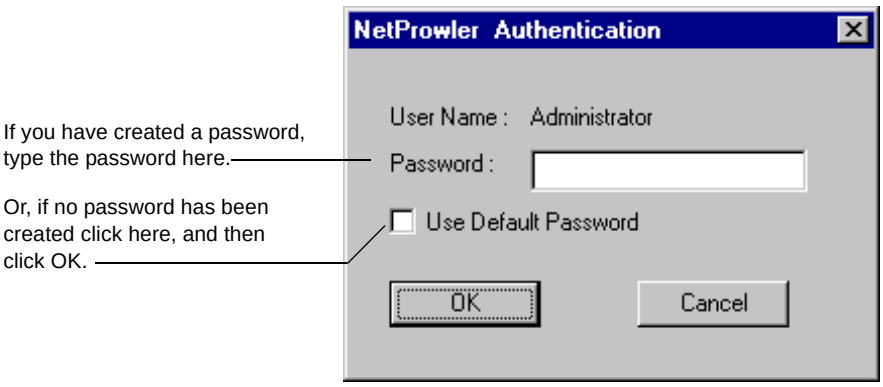

If you have created a password, type the password here.
Or, if no password has been created click here, and then click OK.
NetProwler Authentication
User Name : Administrator
Password :
Use Default Password
OK
Cancel

Figure 3-38: NetProwler Authentication Dialog Box

2. If an administrative password has been created, click in the **Password** box, type the NetProwler administrative password, and then click **OK**.

   Or

   If no password is configured, click the **Use Default Password** check box, and then click **OK**.

The Authentication dialog box appears. AXENT recommends creating an administrative password so that only authorized administrators can modify NetProwler's configuration and view network-based intrusions.

3. Click **Change** to create NetProwler's new administrative password.

   Or

   Click **Continue** to exit.

   The NetProwler Console is stopped, and the system's NIC is taken out of promiscuous mode.

Using NetProwler

Chapter 4: Administering NetProwler

Chapter 5: Building the Address Book

Chapter 6: Configuring NetProwler to Detect Attacks

Chapter 7: Creating Attack Signatures

Chapter 8: Securing Network Resources

Chapter 9: Monitoring Attacks and Network Conversations

Chapter 10: Generating and Viewing Reports

Administering NetProwler

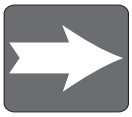
Overview

This chapter contains conceptual and instructional information on how to administer NetProwler. Chapter topics include:

- Updating NetProwler's license
- Changing NetProwler's administrative password
- Importing new attack signatures from AXENT
- Setting up NetProwler's response capabilities
- Setting up applications
- Purging the NetProwler database
- Deleting captured sessions
- Using NetProwler's online help system

Updating NetProwler's License

When you installed NetProwler, you were given a license. The license enables you to use NetProwler for a period of time. Evaluation licenses are usually set at 30 days. After purchasing the software, you must obtain another license. This license may allow you to use NetProwler for the length of your contract period. You should update your NetProwler license prior to it expiring.


TIP

You can view your current license type and the expiration date of your license in the About NetProwler dialog box. Access the About NetProwler dialog box by choosing About NetProwler from the Help menu.

The instructions below describe how to update your NetProwler license.

To update your NetProwler license:

1. If you have not already started NetProwler, do so before continuing.
2. From the Administration menu, choose Update License.

   The Add Licenses dialog box appears
3. In the **License Key** field, type the new 19-character license key.
4. Click **OK**.

   NetProwler updates the license.

Changing NetProwler's Administrative Password

NetProwler stores one administrative password. Out of the box, NetProwler uses a default password. If you leave the default password enabled, anyone can start NetProwler, reconfigure it, and view security-related data. In order to secure NetProwler, AXENT strongly recommends changing the password the first time you run the program. Furthermore, as a general security measure, AXENT advises changing the password regularly.

The following instructions describe how to change the administrative password after you have logged into NetProwler.

To change the administrative password:

1. If you have not already started NetProwler, do so before continuing.
2. From the Administration menu, choose **Change Password**.

   The NetProwler Authentication dialog box appears.

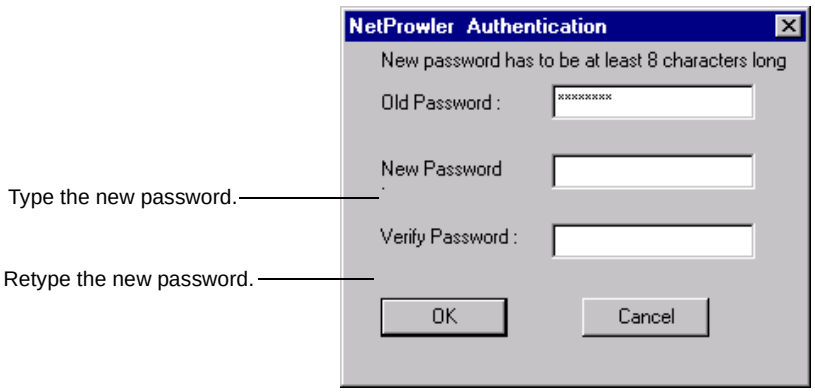


Figure 4-1: NetProwler Authentication Dialog Box

   If you are creating the administrative password for the first time, skip to **Step 4**.

3. Click in the **Old Password** box and type the old password.

If you are creating the administrative password for the first time, the default password will be entered into the Old Password field for you. The default password will be masked by a series of asterisks.

4. Click in the **New Password** box and type the new password.

   Valid passwords must be at least 8 characters long. In addition, the administrative password is case sensitive, allowing you additional password security. The following are examples of valid administrative passwords:

   LeT$GoEat

   AJS45adm

   WeWork4$

5. Click in the **Verify Password** box, and retype the new password.
6. Click **OK**.

   The administrative password is changed.

Obtaining and Importing New Attack Signatures from AXENT

AXENT actively researches new operating system and application security bug reports and hacker attack strategies to develop attack signatures that enable NetProwler to detect and respond to those attempts to exploit known vulnerabilities. You can download these off the AXENT web site, located at:

http://www.axent.com.

The following instructions describe how to download these new attack signatures and import them into NetProwler. After importing them into NetProwler, you will need to activate them for desired systems residing in NetProwler's Address Book.

To obtain and import new attack signatures:

1. Launch a Web browser (e.g., Internet Explorer, Netscape Navigator, etc.), and go to the following URL:

   http://www.axent.com

2. Locate and download the desired attack signatures.
3. If you have not already done so, start or switch to NetProwler.
4. From the Administration menu, choose **Sync New Signatures**.

The Select Attack Signature File dialog box appears.

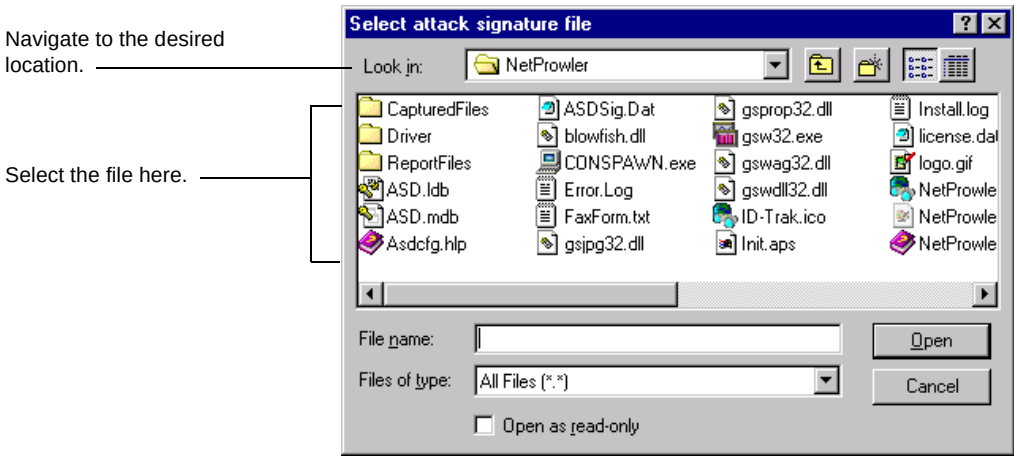


Figure 4-2: Select Attack Signature File Dialog Box

5. Navigate to the location of the downloaded attack signatures, select the desired file, and then choose **Open**.

   NetProwler updates the list of attack signatures.

6. Repeat **Step 8** for each downloaded file.

   The new attack signatures are added to the list. You must associate them with the desired hosts. For instructions on how to associate an attack signature, see *Associating Attack Signatures Manually* on page 6.13.

Setting Up NetProwler's Notification Capabilities

Notification actions notify an administrator (via pager or e-mail) or device (such as a firewall or SNMP Manager) that a security event occurred. The following is a list of notification actions:

- Page a system administrator
- Send e-mail to an administrator
- Notify a Check Point FireWall-1 firewall (The firewall can be configured to respond to that notification by preventing the attacking source from entering the firewall for a period of time, ranging from one minute to forever.)
- Send SNMP traps to SNMP Managers, including Intruder Alert Agents configured to accept and respond to SNMP traps (For instructions on how to configure Intruder Alert to accept and respond to SNMP traps, see the *NetProwler-Intruder Alert Integration Manual* that came with the NetProwler CD-ROM.)

This section describes how to configure NetProwler to interface with the devices that make these notification responses possible. For example, before NetProwler can page an administrator, it must be configured to interface with the computer's modem.

This section does not describe how to configure actions in response to attacks. For instructions on configuring actions in response to an attack, see *Configuring NetProwler Actions* on page 6.19.

Configuring NetProwler to Page

NetProwler can page an administrator in response to a detected attack. NetProwler uses a configured modem device to send the pager notification message to the administrator's paging service. The paging service then pages the administrator.

The instructions below describe how to set up NetProwler to interface with the system's modem. (For instructions on how to configure paging in response to an attack, see *Configuring NetProwler Actions* on page 6.19.)

To configure NetProwler to page:

In the **Configure** tree, choose **Notification Options** and then **Communication Devices**.

The Pager Options box should be visible.

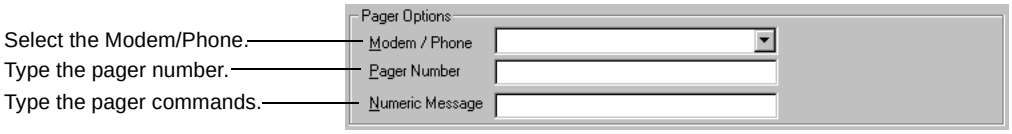


Figure 4-3: Pager Options Box

7. In the **Modem/Phone** box, select the modem that NetProwler will use.
8. In the **Pager Number** box, type the phone number of the Paging service.
9. In the **Numeric Message** box, type the required pager commands.

   If the paging service's answering process requires pauses, use a comma (,) for each required second.

   For example, if your paging service has an automated voice menuing system that requires pauses between each entry, your entry in NetProwler might look something like the following:

   93764897,,,,,,,,,1,,7653797

("9" is used to get an outside line; "3764897" is the paging service's phone number; the commas indicate required pauses; "1" is the menu option allowing you to enter the phone number; and "7653797" is the administrator's phone number. No beginning or ending commands are required.)

10. Click the **Apply** button to save and apply the configuration changes.

    NetProwler is configured to interface with the system's pager; however, NetProwler will not page an administrator until you associate paging with either an attack priority level or specific attack signature / host. For instructions on how to associate pager notification with an attack priority level, see *Configuring Notification Actions by Priority Level* on page 6.22. For instructions on how to configure paging in response to a specific attack on a specific host, see *Configuring Response Actions by Attack Signature* on page 6.24.

Configuring NetProwler to Send E-mail

NetProwler can send an e-mail notification message to a system administrator in response to a detected attack.

The following instructions describe how to set up NetProwler to interface with your mail server and send e-mail.

To configure NetProwler to send e-mail:

1. In the **Configure** tree, choose **Notification Options** and then **Communication Devices**.

   The E-mail Options box should be visible.

Figure 4-4: E-mail Options Box

2. In the **Email Address** edit box, type the destination e-mail address.

   For example, if you want NetProwler to send e-mail to Mark Peterson, your security administrator, type Mark's e-mail address in the E-mail Address edit box. If you want to send this e-mail to more than one person, create a distribution list using your mail server software or configure an e-mail group with the desired recipients, and then insert the name of the list or group in the Email Address box.

3. In the **Mail Server IP Address** edit box, type the IP address of your SMTP mail server.

4. Click **Apply** to save and apply the configuration changes.

   You have configured NetProwler with e-mail capabilities; however, NetProwler cannot send e-mail notification until you associate e-mail with either an attack priority level or attack signature/host. For instructions on how to associate e-mail notification with an attack priority level, see *Configuring Notification Actions by Priority Level* on page 6.22. For instructions on how to configure NetProwler to send an e-mail in response to a specific attack on a specific host, see *Configuring Response Actions by Attack Signature* on page 6.24.

Setting Up NetProwler to Notify a Raptor Firewall

NetProwler can be configured to automatically notify a Raptor® firewall in response to an attack.

NOTE

NetProwler supports firewall hardening on Raptor firewall versions 6.0 and higher with the np_integration_module.exe patch applied. Raptor patches and upgrades are available at:

http://www.raptor.com/cs/FAQ

Upon receiving the NetProwler message, the Raptor firewall can reset the connection or deny access to the attacker depending on how it has been configured. The following graphics illustrate how NetProwler works with the Raptor firewall

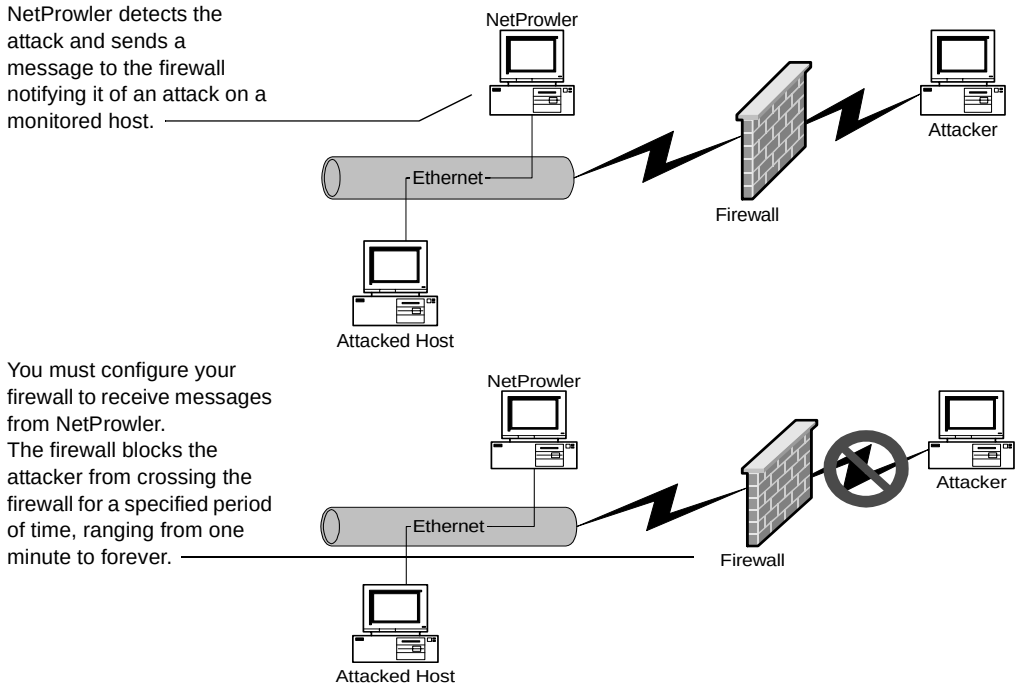

NetProwler detects the attack and sends a message to the firewall notifying it of an attack on a monitored host.
NetProwler
Attacker
Ethernet
Firewall
Attacked Host
You must configure your firewall to receive messages from NetProwler.
The firewall blocks the attacker from crossing the firewall for a specified period of time, ranging from one minute to forever.
NetProwler
Attacker
Ethernet
Firewall
Attacked Host

Figure 4-5: Notifying a Raptor Firewall

NetProwler uses an authenticated, relay-protected UDP protocol to communicate with the Raptor firewall. NetProwler uses a "shared secret" authentication string. "Shared secret" means that both NetProwler and Raptor use the same authentication string. This prevents a third party from inserting or modifying the communication data.

For additional security, the UDP protocol's relay protection prevents a third-party from altering NetProwler or Raptor operations by capturing and re-transmitting the conversation data.

NOTE

You must configure the Raptor Firewall to receive notification messages from NetProwler and respond by terminating the session or denying access to the attacker. For instructions on how to configure the Raptor Firewall to work with NetProwler, visit the following URL:

http://www.axent.com/support2/security/netprowler/raptor.htm

The following instructions describe how to configure NetProwler to send messages to a Raptor firewall.

To configure NetProwler to notify a Raptor firewall:

1. In the **Configure** tree, expand the **Notification Options** branch, and then select **Network Devices**.

The Firewall Options box should be visible.

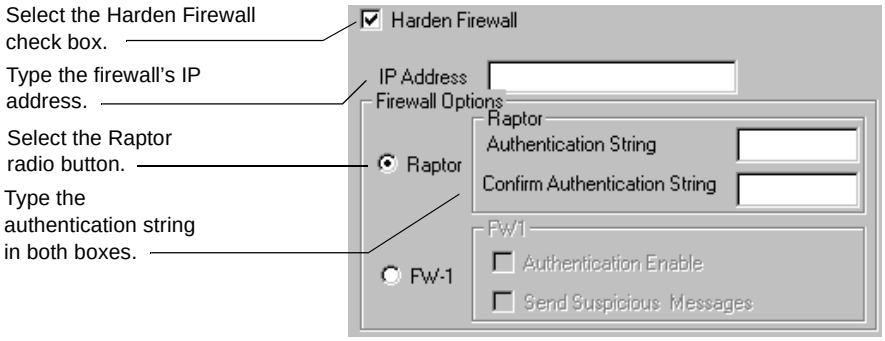


Figure 4-6: Firewall Options Box

2. Select the **Harden Firewall** check box.
3. In the **IP Address** edit box, type the Raptor firewall's IP address.
4. Select the **Raptor** radio button.
5. Type the authentication string in the **Authentication String** box. Then re-type the authentication string in the **Confirm Authentication String** box.
6. Click **Apply** to save and apply the configuration changes.

   You have configured NetProwler with the capability of sending messages to the Raptor firewall; however, NetProwler will not send them until you configure firewall hardening by attack priority level or specific attack signature/host. For instructions on how to configure firewall hardening by attack priority level, see *Configuring Notification Actions by Priority Level* on page 6.22. For instructions on how to configure NetProwler to notify a firewall in response to a specific attack on a specific host, see *Configuring Response Actions by Attack Signature* on page 6.24.

Setting Up NetProwler to Notify a FireWall-1 Firewall

NetProwler can be configured to automatically notify a Check Point® FireWall-1™ firewall in response to an attack. FireWall-1, an Open Platform for Secure Enterprise Computing™ (OPSEC) compliant application, supports integration with other OPSEC compliant systems, such as NetProwler.

NOTE

NetProwler supports firewall hardening on FireWall-1 versions 3.0 and higher.

NetProwler utilizes OPSEC's Suspicious Activity Monitoring Protocol (SAMP) to send messages to FireWall-1 management servers. The SAMP API defines an interface through which a SAMP client—in this case, NetProwler—can send a message to a FireWall-1 management server. SAMP messages sent to the firewall include information about the user's active session. The firewall uses this information to terminate that user's session. The firewall can be configured to disallow entry from the attacker's IP address for a period of time ranging from one minute to forever.

Firewall hardening occurs in two stages. In the first stage, NetProwler detects the attack and responds by sending a SAMP notification message to the FireWall-1 firewall. In the second stage, the firewall performs its configured actions, such as terminating the attacker's session. The following graphics illustrate this process.

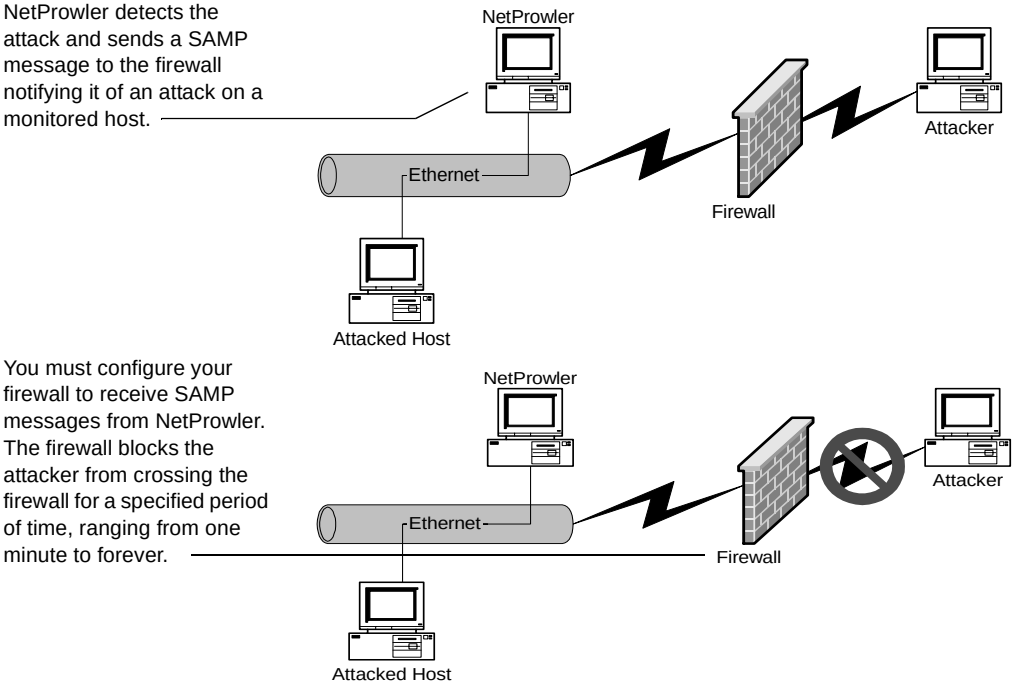

NetProwler detects the attack and sends a SAMP message to the firewall notifying it of an attack on a monitored host.
NetProwler
Attacker
Ethernet
Firewall
Attacked Host
You must configure your firewall to receive SAMP messages from NetProwler. The firewall blocks the attacker from crossing the firewall for a specified period of time, ranging from one minute to forever.
NetProwler
Attacker
Ethernet
Firewall
Attacked Host

Figure 4-7: Notifying a Firewall

You must configure your Check Point FireWall-1 management server with the desired response mechanisms. For instructions on how to configure Check Point's FireWall-1 server to process SAMP messages received from NetProwler, visit the following URL:

http://www.axent.com/support2/security/netprowler/checkpoint.htm

The following instructions describe how to configure NetProwler to send SAMP messages to a specific FireWall-1 firewall.

To configure NetProwler to notify a FireWall -1 firewall:

1. In the **Configure** tree, expand the **Notification Options** branch, and then select **Network Devices**.

   The Firewall Options box should be visible.

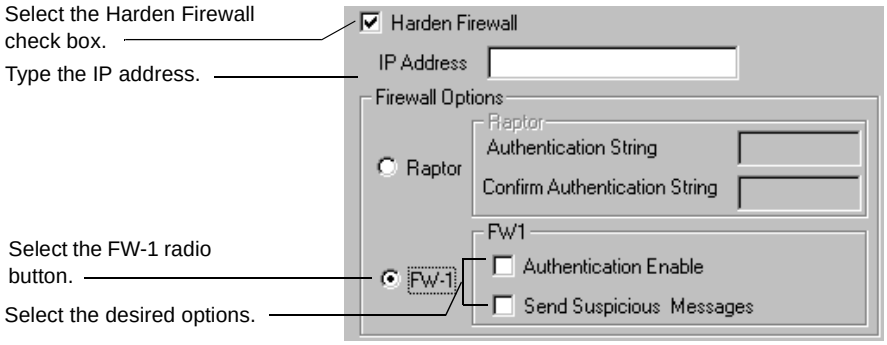


Figure 4-8: Firewall Options Box

2. Select the **Harden Firewall** check box.
3. In the **IP Address** edit box, type the FireWall-1 firewall's IP address.
4. Select the **FW-1** radio button.
5. (Optional) If you want to ensure that NetProwler properly authenticates with the FireWall-1 firewall, then check the **Authentication Enabled** check box. (Recommended)

   If you have checked this box, you must complete the steps for *Configuring FireWall-1 Authentication* on page 4.17.

6. Check the **Send Suspicious Messages** check box.

   This check box works like a switch; with it checked, the option is on; with it unchecked the option is off.

7. Click **Apply** to save and apply the configuration changes.

   You have configured NetProwler with the capability of sending SAMP messages to the desired FireWall-1 firewall; however, NetProwler will not send them until you associate firewall hardening with either an attack priority level or specific attack signature/host. For instructions on how to associate firewall hardening with an attack priority level, see *Configuring Notification Actions by Priority Level* on page 6.22. For instructions on how to configure NetProwler to notify a firewall in response to a specific attack on a specific host, see *Configuring Response Actions by Attack Signature* on page 6.24.

Configuring FireWall-1 Authentication

The following instructions describe how to configure authentication on both the FireWall-1 server and NetProwler host. Both sides must be configured with a "secret key." The secret key allows NetProwler to authenticate with the FireWall-1 server. The following steps should be performed only when you have enabled NetProwler-FireWall-1 authentication. For more information about configuring communication between NetProwler and the FireWall-1 server, see *Setting Up NetProwler to Notify a FireWall-1 Firewall* on page 4.14.

To configure FireWall-1 authentication:

1. On the FireWall-1 Server, open the fwopsec.conf file into a text editor.

   The fwopsec.conf file is located in the \fw\conf\ directory. (On Windows NT systems, this directory is commonly located in the WINNT directory. UNIX systems may vary. You may have to search the file system to locate this file.)

2. Locate either of the following entries:

   sam_server port 18183

   sam_server auth_port 18183

Un-authenticated communication uses the entry sam_server port 18183. The desired setting for authenticated communication is sam_server auth_port 18183.

3. If authorization is disabled, modify the entry as follows:

   sam_server auth_port 18183

4. From the \fw\bin directory, execute the following command:

   fw putkey -opsec <IP Address of the NetProwler Host)

5. When prompted, enter any 8-digit "secret key."

   This authentication key is used by both NetProwler and the FireWall-1 firewall. Remember this key because it will be used in later when configuring authentication on the NetProwler system.

6. Move to the NetProwler system.
7. On the NetProwler host, start the MSDOS Command Prompt utility.
8. Change to the NetProwler directory.

   The default location for NetProwler is:

   <Drive Letter>:\Program Files\NetProwler

9. From the NetProwler directory, execute the following command:

   opsec_putkey -n <IP Address of the NetProwler Host>
   -p <secret key> <IP Address of the FireWall-1 Host>

   For example:

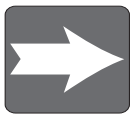
   opsec_putkey -n 194.24.202.86 -p Phoenix1 194.24.202.199

Executing this command generates two files in the NetProwler directory: authkeys.c and rand.c. NetProwler uses these files when sending SAMP messages to the firewall.

Authentication is enabled between NetProwler and the FireWall-1 server.

Configuring NetProwler to Send SNMP Traps

NetProwler can be configured as a Simple Network Management Protocol (SNMP) Agent that sends SNMP traps to SNMP Managers. An SNMP trap is a message that informs the network management system (i.e., SNMP Managers) of some event. Traps are used for informational purposes and do not elicit a response from the receiver. When an attack is detected, NetProwler can be configured to send SNMP traps to up to two SNMP Managers. These Managers can be configured to act on the traps received from NetProwler.


TIP

Because Intruder Alert can be configured as an SNMP Manager, you can integrate NetProwler with Intruder Alert by enabling NetProwler as an SNMP Agent. This allows you to take advantage of the powerful response mechanisms contained in Intruder Alert. To learn how to configure Intruder Alert to receive SNMP traps sent from NetProwler, please refer to *NetProwler-Intruder Alert Integration Manual.*

To configure NetProwler to send SNMP traps:

1. In the **Configure** tree, expand the **Notification Options** branch, and then select **Network Devices**.

The SNMP box should be visible.

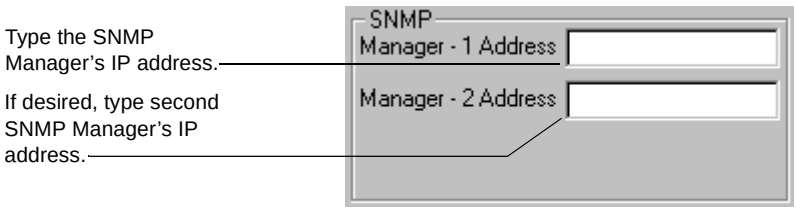

Type the SNMP Manager's IP address.
If desired, type second SNMP Manager's IP address.
SNMP
Manager - 1 Address
Manager - 2 Address

Figure 4-9: SNMP Box

2. In the **Manager-1 Address** edit box, type the IP address of the desired SNMP Manager.
3. (Optional) If you want to send traps to a second SNMP Manager, click in the **Manager-2 Address** edit box and type the IP address of the second SNMP Manager.
4. Click **Apply** to save and apply the configuration changes.

   You have configured NetProwler with the capability of sending SNMP messages; however, NetProwler will not send them until you associate this response mechanism with either an attack priority level or specific attack signature/host. For instructions on how to associate sending SNMP traps with an attack priority level, see *Configuring Notification Actions by Priority Level* on page 6.22. For instructions on how to configure NetProwler to send SNMP traps in response to a specific attack on a specific host, see *Configuring Response Actions by Attack Signature* on page 6.24.

Setting Up Applications

An application is a low-level or end-user program that uses TCP or UDP protocols, such as ftp, telnet, and rLogin. Out of the box, NetProwler comes configured with 70 application types. These applications are stored and configured in the NetProwler Application Book.

NetProwler uses the list of configured applications in two ways:

- To monitor network sessions (e.g., ftp, telnet, Oracle, etc.)
- To scan ports and available services using the Profiler

NOTE

Each application in NetProwler is associated with a "well-known port" as defined in RFC 1700. Please refer to the following URL for more information about well-known port numbers and their associated applications:

http://www.isi.edu/in-notes/rfc1700.txt

In NetProwler, you can add to or delete applications from this list. In addition, if you have modified an application to communicate on a non-standard port, you can modify the application's configuration to monitor the application on that port.

Topics in this section describe how to add to, delete from, and modify applications in the Application Book.

Adding an Application

To add an application:

1. In the **Configure** tree, choose **Application Book**.

   The list of applications should be visible.

2. Click **Add New**.

   The Application Book Entry dialog box appears.

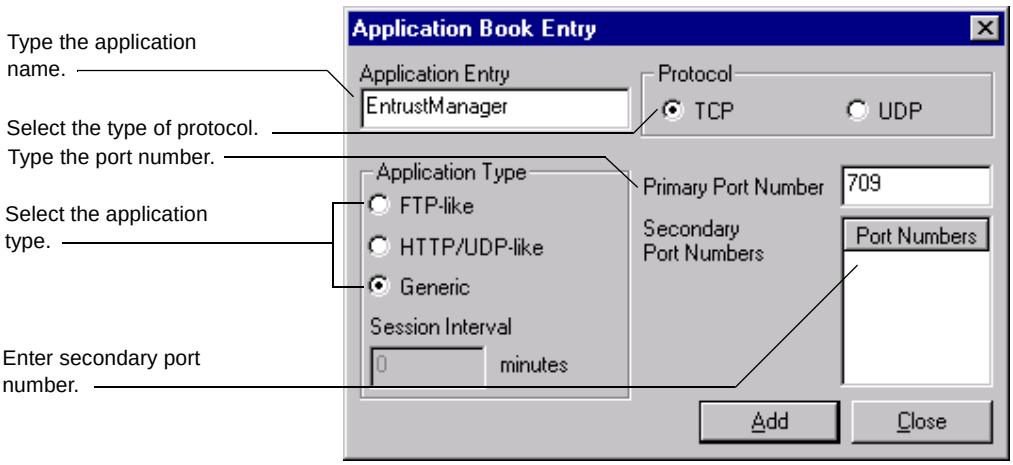


Figure 4-10: Application Book Entry Dialog Box

3. In the **Application Entry** field, type the name of the application.
4. In the **Application Type** box, select the application type.

The following table describes each option and how to configure it if necessary.

Type	Description
FTP-like	FTP-like applications use 2 channels, one for data and one for control, in effect commands from client or server.
HTTP / UDP-like	HTTP / UDP-like applications use many little sessions rather than one standard session.
Generic	Generic applications use the same session from start to finish such as telnet, in effect one client port and one server port for the entire session.

Table 4-1: Application Type Description

5. In the **Protocol** box, specify the type of protocol the application uses.
6. In the **Primary Port Number** field, type the primary port number.
7. In the **Secondary Port Numbers** box, click in the upper left-hand corner of the box (until an entry box appears), and type the number of the secondary port.
8. Repeat **Step 7** for additional port numbers. (Click just below the previous number to access the entry box.)
9. Click **Add**.

   The application is added to the Application Book.

10. Repeat **Steps 3–9** for additional applications.
11. When finished adding applications, click **Close**.
12. Click **Apply** to save and apply the changes.

Deleting an Application

To delete an application:

1. In the **Configure** tree, choose **Application Book**.
2. Click the desired application in the list (so that it is highlighted), and then click **Delete**.

   Or

   Right-click the desired application, and then choose **Delete**.

   The application is removed from the list.
3. Click **Apply** to save the changes.

Modifying an Application

After an application has been created, you can modify its configuration.

To modify an application:

1. In the **Configure** tree, choose **Application Book**.
2. Right-click on the desired application in the list, and then choose **Modify**.

   (You can also double-click on the desired application in the list.)

The Edit Application Book Entry dialog box appears.

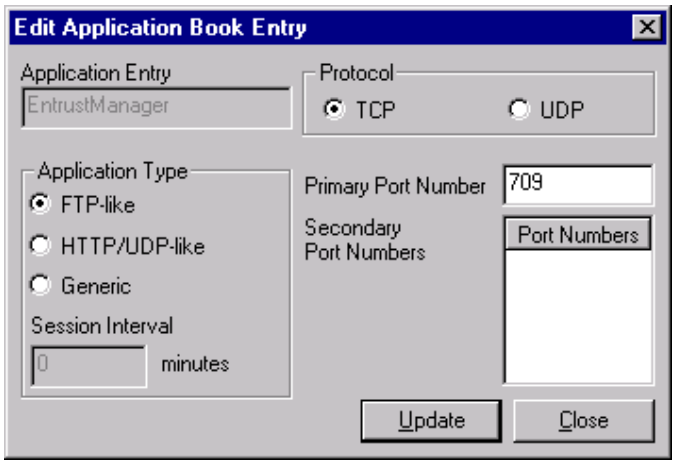


Figure 4-11: Edit Application Book Entry Dialog Box

3. Make the desired changes, and then click **Update**.
4. On the **Configure** window, click **Apply** to save the changes.

   The changes are activated in NetProwler.

Purging the NetProwler Database

When an attack occurs, NetProwler records it in the NetProwler database. The NetProwler database is based on the Microsoft Access database (.mdb) format. If NetProwler was installed in the default location, the NetProwler database is stored in the <*Drive Letter*>:\Program Files\NetProwler directory. The name of the database is "NetProwler.mdb."

Over time, the information in the database becomes out dated and otherwise unnecessary. If you want to retain this information, archive the Netprowler.mdb file, and then purge the desired information from the database. The Purge function deletes data older than a specified date. The Purge function does

not purge configuration information—only logged alert details. The following instructions describe how to purge information from the NetProwler database.

To purge the NetProwler database:

1. (Optional) Backup the NetProwler.mdb database.

   (You should exit NetProwler before you backup the database. You can corrupt the database if you attempt to back it up while NetProwler is writing to it.)

2. On the NetProwler toolbar, click **Purge**.

   The Purge Database dialog box appears.

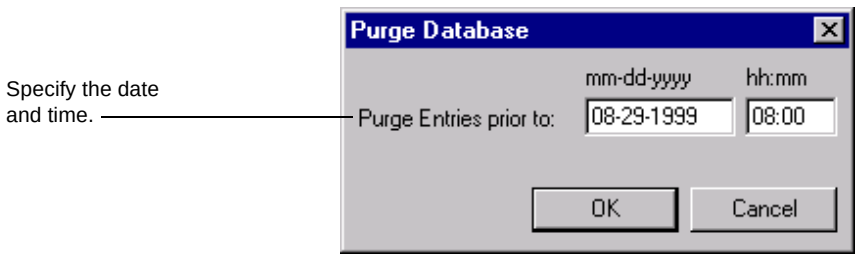


Figure 4-12: Purge Database Dialog Box

3. Specify the date and time, and then click **OK**.

   Entries older than the specified date and time will be deleted.

   If you are deleting all entries in the database, the following information dialog appears.

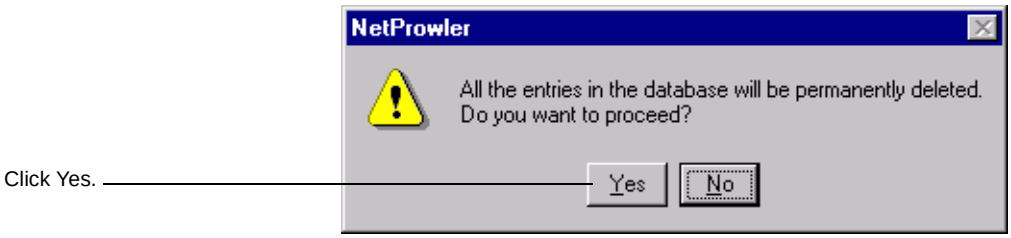


Figure 4-13: NetProwler Information Dialog Box

4. Click **Yes**.

   The records are permanently removed from the database.

Deleting Captured Sessions

When NetProwler captures a session, it creates a text file where it can store the contents of the session. If NetProwler was installed in the default location, these session files are stored in the <*Drive Letter*>:\Program Files\NetProwler\CapturedFiles directory. When you no longer need to view a captured session, you can delete the file from the directory.

Using Online Help

NetProwler offers an online help system to assist you as you use this product. The following sections describe how to access and use Help.

Entering Help

You can access help in the following ways:

- Choose Help Contents from the Help menu
- Clicking the Help Button in a dialog box
- Pressing F1 in a dialog box

If you access Help from the Help menu, there are three ways of locating the topics you want: Contents, Index, and Find. These methods of locating topics correspond to the three tabs on the NetProwler 3.0 Help window.

Each method is described in the following table.

Tab	Description
Contents	The Contents tab contains a hierarchical listing of topics, organized much like the table of contents in a book.
Index	The Index tab contains a list of words or phrases either contained in the help file or designed to help you find topics (synonyms or program terms, features, etc.).
Find	The Find tab lets you search for words found in topics in the help file.

Table 4-2: Help Tab Descriptions

Help Conventions

The following table describes the conventions used in online help.

Convention	Description
#	Numbers precede instructions for you to carry out when completing a task.
Note:	Bold text is used for notes, hints, warnings, etc.
	Buttons like this can be clicked to jump to other topics. In some cases when you click a button, you may see a list of several topics; double-click any topic in the list to display that topic.
Jump	Green text with a solid underline can be clicked to jump to another topic.
Popup	Green text with a dotted underline can be clicked to open a popup window.
	This icon indicates a link to a specific location on the Internet. When you click this icon, the Help system launches your default Internet browser and takes you to a specific URL.

Table 4-3: Conventions Used in Online Help

Chapter 5

Building the Address Book

Overview

NetProwler monitors configured hosts in a network segment. These hosts must be listed and activated in NetProwler's Address Book. The most efficient way to add systems and devices to the Address Book is to use the Profiler configuration tool. The Profiler automates the process by scanning the network for "live" systems and devices. When the Profiler identifies a live system, it scans the system against the list of defined applications / ports to see what services are available on that system. After performing the port scan, it adds that system to the list of potential systems to monitor. Once you have identified the systems that are active in the network segment, you can associate the desired attack signatures with each system and then add those systems to the NetProwler Address Book.

In addition to the automated Profiler, NetProwler lets you add and delete systems to the Address Book manually. (If you add them manually, you will have to manually configure each system with the list of desired attack signatures.)

In this chapter, you will learn how to add systems to the Address Book by using the Profiler and by manually entering systems in.

Profiling a Network

NetProwler monitors systems for associated attacks. Addressing the needs of time-pressed security administrators or those with little security expertise, the Profiler offers the most efficient means for quickly and easily configuring NetProwler. The Profiler:

- Identifies, if possible, live systems and devices on the network.
- Identifies, if allowed, the type of operating system running on the host.
- Provides quick and easy configuration of attack signatures. (NetProwler automatically suggests a list of attack signatures to associate. You can add to or subtract from this list, and then enable the system.)
- Builds NetProwler's Address Book. (NetProwler monitors only the systems configured in this book.)
- Keeps NetProwler up-to-date with network configuration changes. (You can configure NetProwler to reprofile the network at regularly scheduled intervals. For instructions on how to schedule the Profiler to run at regular intervals, see *Scheduling the Profiler* on page 5.13.)

The Profiler works by scanning a range of IP addresses to locate "live" systems on the network. (A live system is one that responds to an ICMP echo request.) After identifying a live system, the Profiler determines what services are available on that system. It then adds that system to the list of systems awaiting configuration and additionally to the Address Book. With systems now in the list, you can associate the desired attack signatures with each system and add them to the Address Book. Once a system is in the Address Book, NetProwler begins monitoring that system for associated attacks.

In environments using Dynamic Host Configuration Protocol (DHCP), AXENT recommends that you manually enter the systems configured with DHCP as a range (or series of ranges) with all attack signatures applied to that range. This is because hosts identified and configured by NetProwler's Profiler will change when those hosts' DHCP-assigned IP address expires. For instructions on how to manually add an entry to the Address Book, please refer to *Adding Systems to the Address Book Manually* on page 5.16.

You can also profile the network and build an address book by using the Profiler Schedule. The Profiler Schedule provides an advantage over running the Profiler from the toolbar. During a scheduled profile, if the Profiler finds a system that does not already exist in the Address Book, it will automatically associate the selected common attack signatures and all other attacks that apply to that system's type of operating system and available services and then add it to the Address Book. For more information on using the Profiler scheduling feature, see *Scheduling the Profiler* on page 5.13.

The following sections describe how to start the Profiler and enable systems in the Address Book and associate them with attack signatures.

Starting the Profiler

The Profiler scans the network for live systems. To configure the Profiler, you will:

- Specify the range of IP addresses to scan
- Select Common Attacks (i.e., Port Scan, Ping of Death, etc.) to automatically associate with detected hosts
- Define the amount of time before a system is determined inactive or unreachable

- Define the amount of time before ports on the detected system are determined inactive
- Select a default operating system

After you have configured and then started the Profiler, it will begin scanning the network for live systems and devices. When it finds a system, it adds it to the list of systems awaiting configuration. (These systems are initially listed as "Not Enabled." Not Enabled means that the system has not been configured with attack signatures and added to the Address Book.) Instructions for configuring systems are discussed in the section *Configuring a Profiled System* on page 5.6.

The following instructions describe how to configure and start the Profiler.

To Configure and Start the Profiler:

1. In the **Configure** tree, select **Profiler**.

   The Profiler Results box should be visible.

2. On the NetProwler toolbar, click **Profile Now**.

   The Start Scan dialog box appears.

Specify the range of IP addresses.

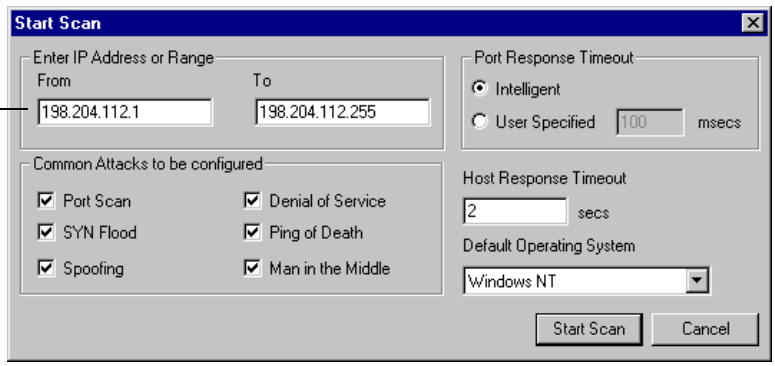


Figure 5-1: Start Scan Dialog Box

3. In the **From** edit box, type the starting IP Address, and then press **Tab**.

The first three octets of the IP address appear in the To box.

4. In the **To** box, type the ending IP address.
5. In the **Common Attacks to be Configured** box, check or uncheck the common attacks that will be associated with detected systems.
6. In the **Port Response Timeout** box, select **Intelligent** for the most efficient method of determining live ports. NetProwler dynamically sets the response timeout depending on the actual response time of the network. (Recommended)

   Or

   To specify a maximum number of milliseconds spent on each port before concluding that no service is available on that port, select the **User Specified** radio button, and then type the number of milliseconds.

   (Experience will dictate whether or not NetProwler needs more time while scanning ports.)
7. In the **Host Response Timeout** box, specify the number of seconds before NetProwler will determine that no host exists on that IP address or the host is unreachable.

   You should consider increasing the number of seconds if you are scanning during high volume periods.
8. In the **Default Operating System** edit box, select the default type of operating system.

   This information is used when NetProwler suggests attack signatures for activation on the selected system. If NetProwler can not automatically determine the type of operating system, it assumes that it is the default.
9. Click **OK**.

   The Profiler begins scanning the specified range of hosts. Active systems will be added to the list of systems to enable. For instructions on how to enable a system, see *Configuring a Profiled System* on page 5.6.

After the Profiler has scanned the specified range of IP addresses, the following information dialog will appear.

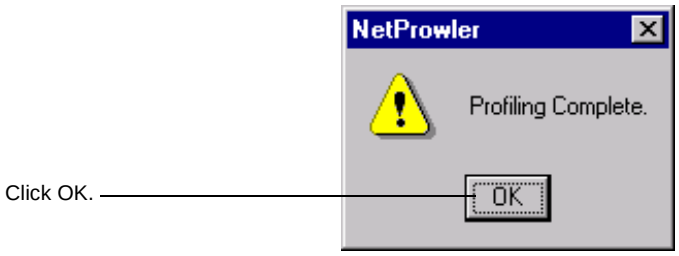


Figure 5-2: NetProwler Dialog Box

10. Click **OK**.

    NetProwler has finished profiling the range of IP addresses.

Configuring a Profiled System

After the Profiler has identified a live system on the network, it adds it to the Profiler Results list. Initially, these systems are classified as "Not Enabled." A system becomes enabled after you modify the list of detected applications and associate desired attack signatures with the system. After configuring the systems, you can add them to the NetProwler Address Book. Once the system is added to the Address Book, NetProwler begins monitoring the system for the associated attacks.

The following instructions describe how to configure profiled systems and add them to the Address Book.

To configure a profiled system:

1. If you have not already started and run the Profiler, do so before continuing.

   For instructions on how to start the Profiler, see *Starting the Profiler* on page 5.3.

2. In the **Configure** tree, select **Profiler**.

3. In the **Profiler Results** box, select the desired system, and then click the **Configure** button.

   The Host Details dialog box appears. This box lists the applications detected when the system was scanned.

These are the services the Profiler detected during the scan. Uncheck services to exclude them from being monitored.

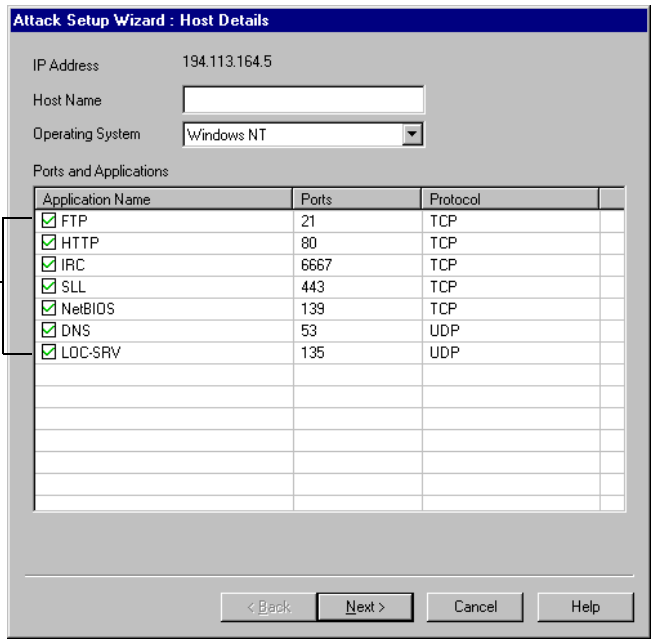


Figure 5-3: Host Details Dialog Box

4. (Optional) In the **Host Name** box, type the name of the system it is incorrect.

5. (Optional) In the **Operating System** drop-down list box, select the system's operating system type, if the selected operating system is incorrect.

6. (Optional) In the **Ports and Applications** table, uncheck the applications and ports you do not want NetProwler to monitor, and then click **Next**.

   The Ports and Applications list is used to suggest which attack signatures to associate with the selected system. For example, if HTTP is checked, NetProwler will suggest associating the *Apache Web Server Denial of Service*

Attack and other HTTP-related attack signatures with the selected system. If you realize that an application is active but should be disabled, uncheck the application in this box, and then disable the application on the server at a later time.

The Edit Attack Association dialog box appears.

NetProwler suggests attack signatures to apply based on the detected operating system.

Select the attack and click here to remove the attack signature.

To view or modify an attack's configuration, select the attack in the list and then click Details.

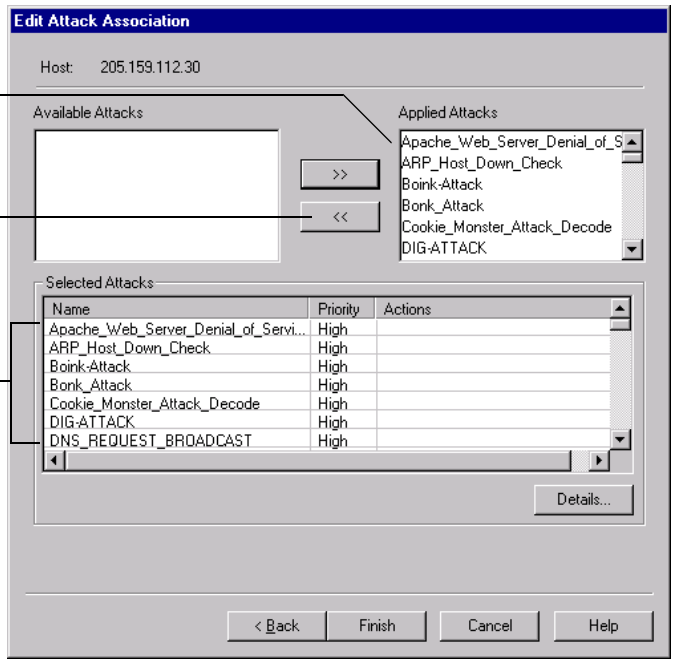


Figure 5-4: Edit Attack Associations Dialog Box

NetProwler suggests a list of attack signatures to apply based on the detected operating system and checked applications.

7. (Optional) Remove attack signatures by selecting the attack signatures in the **Applied Attacks** box and then clicking the **Back Arrow** button.

8. (Optional) To modify an attack signature's configuration, such as configuring authorized hosts (hosts that are allowed to access a monitored resource without NetProwler reporting an attack.) and attack response mechanisms, select the attack signature in the **Selected Attacks** box, and then click **Details**.

   For help and instructions on modifying an attack signature's configuration, click the Help button or see *Modifying an Attack Signature (from within the Profiler)* on page 5.11.

9. (Optional) Repeat **Step 8** to modify additional attack signatures.

10. Click **Finish**.

11. When finished, click **Apply** to save the configuration changes.

    The selected systems are configured with attack signatures and added to the Address Book. NetProwler will immediately begin monitoring the configured systems.

Removing (Disabling) a Configured System

After profiling a system and configuring it, you can remove or disable the system's configuration. A removed or disabled system will not be added to the NetProwler Address Book when Apply is pressed. If the system has already been added to the Address Book but you want to remove it, you will have to manually remove it from the Address Book.

If you already configured the system and then clicked Apply, the system was added to the Address Book. If this has occurred and you want to remove the system from the Address Book, you will have to manually delete it. For instructions on how to delete the entry from the Address Book, see *Deleting Systems from the Address Book* on page 5.19. (You cannot delete an entry from the Profiler Results list.)

To disable a configured system:

1. In the **Configure** tree, select **Profiler.**
2. Select the desired system in the **Profiler Results** list, and then click **Disable Configuration**.

   Or

   Right-click on the desired system, and then select **Disable Configuration**.

   The selected system is marked as "Not Enabled." It will not be added to the Address Book when you click Apply.

3. Click **Apply** to save the changes.

Modifying an Attack Signature (from within the Profiler)

Before associating an attack signature on a system, you can:

- Change the attack signature's priority level
- Define authorized sources of the attack (Alarms will not be logged or actions taken when authorized users trigger the attack signature.)
- Configure notification and response actions

Modifying the attack signature in the Profiler performs the same function as modifying in the Configure, ASD, Attack Association section of NetProwler. The ability to modify the attack signature while in the Profiler was added for last minute configuration or configuration viewing prior to applying the attack signature.

To modify an attack signature:

1. If you have not already started and run the Profiler, do so before continuing.

   The Profiler will build the list of systems in the Profiler Result box.

2. Select a system in the **Profiler Results** box, and then click **Configure**.

   Or

   Select the system in the **Profiler Results** box, right-click on the desired system, and then select **Configure**.

   The Host Details dialog box appears.

3. Click **Next**.

   The Edit Attack Association dialog box appears.

4. Select the desired attack signature in the **Selected Attacks box**, and then click **Details**.

   The Edit Attack Association Details dialog box appears.

5. Select the desired options.

   The following table describes how to perform each function.

To	Do This
Allow authorized users access to a monitored resource on a port or ports without NetProwler reporting an attack.	Locate the host in the Authorized box and check its check box. (If the attack stems from an authorized source, no alarm or response will trigger.)
Configure which applications are associated with this attack	In the Applications box, check the associated applications.
Select which action mechanisms to trigger when an attack is detected	Check the desired notification and response actions in the Action box. (NetProwler must also be set up with the capabilities to send e-mail, page, send SNMP traps, and harden a firewall.)
Change the attack signature's priority level	Select the desired priority (High, Medium, or Low) in the Priority drop-down list box.

Table 5-1: Modification Options

6. When finished modifying the attack signature, click **Update**.
7. On the **Edit Attack Association** dialog box, click **Finish**.
8. Click **Apply** to add the system to the Address Book and have NetProwler begin monitoring the configured systems.

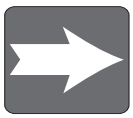
Scheduling the Profiler

Information systems and network configurations change constantly. Computers and network devices get added to, moved around, or removed from the network on a regular basis. Any node-based configuration process can be time consuming; therefore, NetProwler has been designed with a scheduling tool that allows you to automatically reprofile or rescan the network for changes. Reprofiling the network tells you which systems are now “live” or have been added since the last scan.The Profiler stores only one continuous range of IP addresses.

In Dynamic Host Configuration Protocol (DHCP) environments, AXENT recommends manually entering DHCP systems as a rang or series of ranges and associating attack signatures with those ranges. For more information about manually entering ranges of systems, see *Adding Systems to the Address Book Manually* on page 5.16.

If the Profiler finds a system that does not already exist in the Address Book, it will automatically associate the selected common attack signatures and all other attack signatures, including user-defined attack signatures, that apply to that system’s type of operating system and available services, and then add the system to the Address Book.

If the Profiler finds a system that already exists in the Address Book and it is configured with selected attack signatures, it will leave its Address Book configuration intact, but adds any attack signatures applied through the scheduled profiling.



You can configure NetProwler to automatically configure itself to monitor network systems and devices by setting a scheduled profile to start immediately.

The following instructions describe how to configure NetProwler to reprofile the network at regularly scheduled intervals.

To schedule the Profiler:

1. In the **Configure** tree, select **Profiler**.

   The Schedule box should be visible.

2. Click **Change**.

   The Profiler Schedule dialog box appears.

Specify the range of IP addresses.

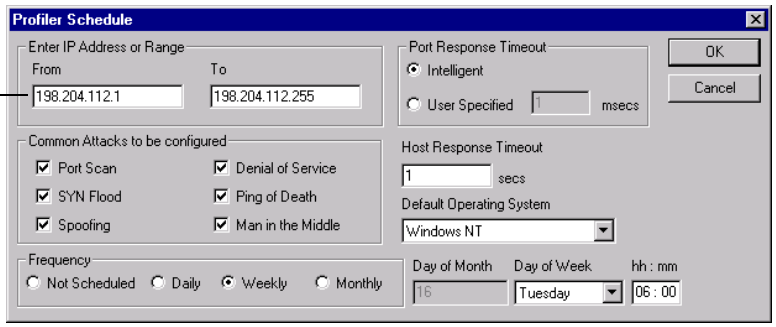


Figure 5-5: Profiler Schedule Dialog Box

3. In **From** edit box, type the starting IP Address, and then press **Tab**.

   The first thee octets of the IP Address appear in the To box.

4. In the **To** box, type the ending IP address.

5. In the **Common Attacks to be Configured** box, check or uncheck the common attacks that will be associated with detected systems.

6. In the **Frequency** box, select the desired frequency.

7. Specify the desired time of day, day of week, or month of day based on the selected frequency.

If you selected Daily, only the HH:MM field will be available. Similarly, if you selected Weekly, the Day of Week and HH:MM fields will be available. And if you selected Monthly, the Day of Month and HH:MM fields will be available.

8. In the **Port Response Timeout** box, select Intelligent for the most efficient method of determining live ports. (Recommended)

   Or

   To specify a maximum number of milliseconds spent on each port before concluding that no service is available on that port, select the **User Specified** radio button, and then type the number of milliseconds.

   (Experience will dictate whether or not NetProwler needs more time while scanning ports. If a host is not detected by the Profiler due to a slow network link, this timeout can be adjusted to force the Profiler to wait longer before timing out.)

9. In the **Host Response Timeout** box, specify the number of seconds before NetProwler will determine that no host exists on that IP address or the host is unreachable.

   You should consider increasing the number of seconds if you are scanning during high volume periods.

10. In the **Default Operating System** edit box, select the default type of operating system.

    This information is used when NetProwler suggests attack signatures for activation on the selected system.

11. Click **OK**.

    The Profiler will rescan the specified range of hosts at the selected time.

Adding Systems to the Address Book Manually

You can add systems and devices to the Address Book manually. You can enter systems one at a time or specify a range of systems to add. In NetProwler, a range is a group of systems configured as a single system—all systems within the specified range are treated the same; they would have the same attack signatures applied with them.

In environments using Dynamic Host Configuration Protocol (DHCP), systems are constantly renewing their IP addresses. If you configured your environment using the Profiler, the configuration will soon be incongruent with the actual environment. This could potentially yield high numbers of false positive alarms. To avoid this, you can manually configure DHCP systems as ranges. For example, let's say you have a Class C network 155.202.12.1 to 155.202.12.255, and numbers 100 through 200 represent the DHCP pool. Therefore, you could create one entry as a range. The range would be defined as all systems from 155.202.12.100 through 155.202.12.200. After creating the range, you would need to manually configure the range with the desired attack signatures. For instructions on how to manually configure a system with attack signatures, see *Associating Attack Signatures Manually* on page 6.13.

Adding a Single System

A single system will have its own associated attack signatures.

To add a single system:

1. In the **Configure** tree, choose **Address Book**.
2. Click **Add New**.

The Address Book Entry dialog box appears.

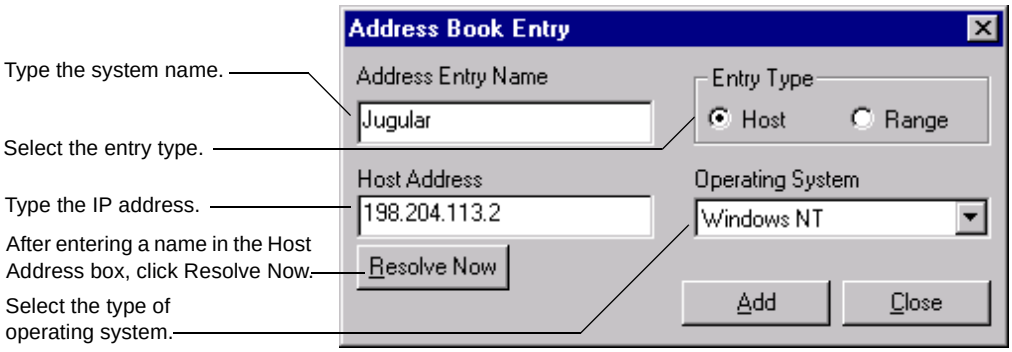


Figure 5-6: Address Book Entry Dialog Box

3. In the **Address Entry Name** edit box, type the name of the system.
4. If it is not already selected, select the **Host** radio button.
5. In the **Host Address** edit box, type the system's IP address.

   Or

   Type the name of the system, and then click **Resolve Now**.

   NetProwler performs a reverse DNS lookup to verify that the system resides in the DNS table.
6. In the **Operating System** drop-down list box, select the system's operating system

   When you configure attack signatures for this system, NetProwler will suggest a list of attack signatures based on the type of operating system selected here.
7. Click **Add**.

   The system is added to the Address Book.
8. Click **Apply** to save and apply the changes.

Adding a Range of Systems

NetProwler allows you to enter a range of systems as a single entry. All systems within the range are treated the same; they will have the same attack signatures associated with them.

NOTE

If a system appears as a single entry in the Address Book, it will have its own set of applied attack signatures. If the same system also exists within a range of IP addresses, then it may have a different set of applied attack signatures. If the same attack signature is applied to both entries, then NetProwler will report the attack twice.

To add a range of systems:

1. In the **Configure** tree, choose **Address Book**.
2. Click **Add New**.

   The Address Book Entry dialog box appear
3. In the **Address Entry Name** edit box, type the name of the system.
4. Select the **Range** radio button.

   The Start Address and Ending Address fields appear.

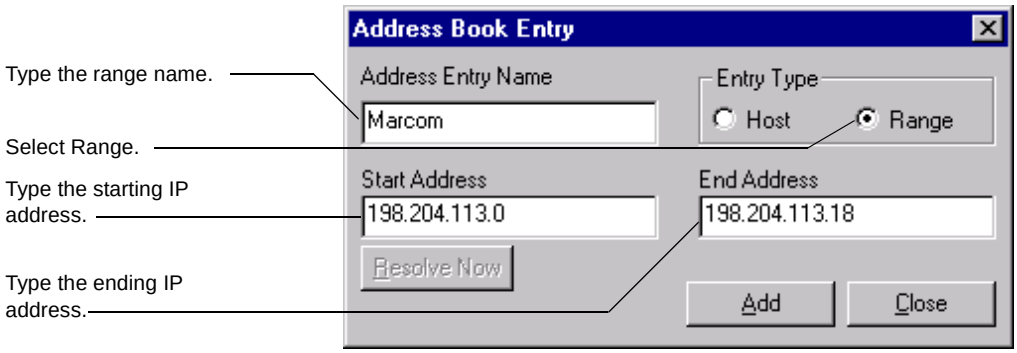


Figure 5-7: Address Book Entry Dialog Box

5. In the **Start Address** box, type the starting IP address, and then press **Tab**.
6. In the **End Address box**, type the ending IP address.
7. Click **Add**.

   The range is added to the Address Book. You must configure the range with associated attack signatures. For instructions on configuring the range with associated attack signatures, see *Associating Attack Signatures Manually* on page 6.13.

8. Repeat **Steps 3–7** for additional entries.
9. When finished, click **Close**.
10. Click **Apply** to save and apply the changes.

Deleting Systems from the Address Book

After a system or range of systems have been added to the Address Book, you can delete them.

To delete an entry from the Address Book:

1. If you have not already done so, in the **Configure** tree, select **Address Book**.

   Entries in the Address book should be visible.

2. Select the desired entry, and then click **Delete**.

   The entry is deleted from the Address Book.

3. Click **Apply** to save and apply the changes.
4. Click **Yes** at the confirmation box.

   NetProwler deletes the entry from the Address Book.

Configuring NetProwler to Detect Attacks

Overview

An attack signature is a uniquely identifying action or series of actions that identify a type of attack. Attack signatures are at the heart of NetProwler. NetProwler comes with numerous preconfigured attack signatures ready for activation. In addition to these preconfigured attack signatures, you can create your own attack signatures with NetProwler's Attack Signature Definition tool and import AXENT provided attack signature updates.

When NetProwler detects an attack, it immediately displays the event as an Alarm in the NetProwler console. In addition to this standard notification mechanism, you can configure additional mechanisms, including resetting the session, executing a command or batch file, capturing the session for analysis, paging an administrator, and more.

In this chapter, you will learn:

- About NetProwler's predefined attack signatures
- How to manually associate an attack signature with a system
- How to remove an associated attack
- How to configure NetProwler's response mechanisms

Understanding Attack Signatures

An attack signature is a uniquely identifying action or series of actions that identify an attacker's malicious behavior. An attack signature is to security administrators as fingerprints are to criminal investigators.

In NetProwler, attack signatures can be grouped into three categories: Common, custom, and user-defined.

Common Attacks Signatures

A "Common" attack signature is an attack signature that is known and frequently used on one or more popular operating systems. NetProwler comes with six "Common" attack signatures. These six attack signatures can be associated with any system or device on the network that has an IP address.

Common attacks are not session based, meaning that the attacking system does not require an established connection to carry out the attack. Therefore, there is no way to disconnect or reset a session when these attacks are detected.

The following sections describe NetProwler's six Common attacks.

Port Scan

Network probe tools, such as AXENT's NetRecon, perform port scans to gather information about potential security vulnerabilities. While port scanning is a legitimate and useful tool for system administrators, it may indicate the presence of an attacker trying to gather information about a system. By scanning ports, an attacker can identify the services available on a system and use that information to exploit the system.

By default NetProwler detects this attack after 20 ports have been scanned within a 60-second period. You can modify this threshold if desired. For instructions on how to modify the Port Scan threshold, see *Adjusting the Port Scan Threshold* on page 6.8.

SYN Flood

Many computers using TCP/IP are susceptible to a denial of service attack called SYN flooding. This attack takes advantage of the "three-way handshake" network connection protocol, where a connection request (synchronization request or SYN) packet is sent to a remote system. The remote system replies with a response packet (known as a synchronization acknowledgment packet or SYN/ACK). Finally, the local system confirms with an acknowledgment (or ACK) packet. The following graphic illustrates this process.

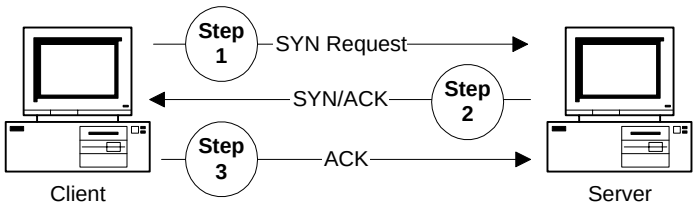


Figure 6-1: TCP Three-way Handshake

A SYN flood involves sending a large number of SYN packets, typically with a spoofed source address. In turn, the attacked host sends out SYN/ACK packets and then waits for the acknowledgment packets to return, but they never arrive. This denial of service type attack can slow down the computer and

network being attacked, and tie up all available TCP connections on the attacked system, preventing legitimate connections from occurring.

By default, NetProwler logs the alarm if eight half-open connections are detected. When detected, NetProwler attempts to reset those eight half-open connections. (It sends eight packets with the Reset flag set.) This closes eight packets and attempts to prevent a denial of service. This SYN Flood threshold can be adjusted. For instructions on how to adjust this threshold, see *Adjusting the SYN Flood Threshold* on page 6.9.

Denial of Service

NetProwler detects a ping flood denial of service attack. A ping command option allows remote users to repeatedly ping a host. The attack pings and keeps pinging a remote system as fast as the attacking computer can process the ping command. Once invoked, this process will continue until it is physically stopped. In addition, if an attacker can log on to other systems (via telnet, rlogin, etc.) they can barrage the target host from that system as well. The target host spends most or all of its time responding to ICMP Echo requests, which slows down or denies legitimate users trying to gain access to that network resource. The intent of this type of attack is to handicap or cripple the target host.

By default, if an alarm is logged NetProwler detects 5 denial-of-service packets (ICMP Echo requests) within a 15 second period of time. This threshold can be adjusted. For instructions on how to adjust the Denial of Service threshold, see *Adjusting the Denial of Service Threshold* on page 6.9.

TCP/IP Spoofing

A TCP/IP spoofing attack is a complex attack that exploits a trusted relationship between two systems. Essentially, an attacker uses a trusted system to gain access to a target system. Through a series of complex steps, the attacking system appears as the trusted system in order to gain access to the target.

For an excellent description of TCP/IP spoofing and how it works, see *IP-spoofing Demystified: Trust Relationship Exploitation* at the following URL:

http://www-phys.rrz.uni-hamburg.de/provos/security/ph48.txt

NetProwler detects this attack by identifying packets sent from outside the Local Area Network (LAN) that purport to be from within the LAN. Because of the nature of your network's configuration, this may cause false positive alarms. Therefore, you may need to adjust how NetProwler detects this attack. For more information about how to adjust the TCP/IP Spoofing settings, see *Adjusting the TCP/IP Spoofing Settings* on page 6.10.

Ping of Death

The Ping of Death attack is an attack that sends an oversized ping packet to target system. When the target system receives the packet, it overflows the system's buffer, resulting in varying effects, including crashing, rebooting, and hanging the system.

The Ping of Death attack is a serious problem because it can be easily reproduced. The Ping of Death attack is executed as easily as sending the following command:

ping -l 65510 <system's IP address>

(The IP header [20 bytes] combined with the ICMP header and ping information [8 bytes] plus 65510 bytes creates an oversized [larger than 65535 bytes] ping packet. If you want to test this on your system, note that Microsoft corrected this problem in Service Pack 3 [SP3] on Windows NT systems. Unless you load an older implementation of ping on these systems, you will not be able to duplicate this attack from a Windows NT system with SP3.)

Most implementations of ping won't allow an invalid ping datagram to be sent. The best insurance against the Ping of Death attack is to patch the operating system. See your operating system vendor to see if your system is protected against this type of attack.

NetProwler allows you to define the adjust the size of the ping packet requirements. For instructions on how to adjust these Ping of Death settings, see *Adjusting the Ping of Death Settings* on page 6.12.

Man in the Middle

The Man-in-the-Middle attack is a sophisticated session-based attack where the intruder hijacks an established communication link. The intruder intercepts messages from the sender and then substitutes them with messages of his own. For example, an attacker might watch an Internet-based banking site that provides bill paying services. As clients visit this site, the attacker diverts the bank's responses. Using a malicious applet that mimics that bank's legitimate service, the attacker steals the users credit card and bank account numbers. The following graphic illustrates the Man-in-the-Middle attack.

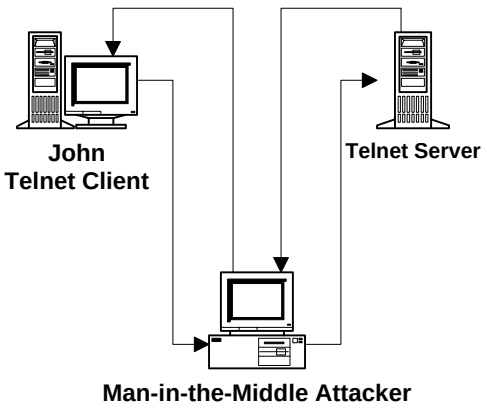


Figure 6-2: Man-in-the-Middle Attack Diagram

The man in the middle fools both the client and the server into thinking that they are talking to each other, while they are really communicating with the attacker.

NetProwler can detect when a communication session has been hijacked by a third party, but it can only detect this for applications configured in the Application Book.

No adjustments are necessary with this attack signature.

Custom Attacks Signatures

NetProwler 3.0 comes with a number of preconfigured "custom" attack signatures. Custom attack signatures are hard coded in NetProwler so that the detection criteria cannot be modified by users. However, you can define:

- Authorized sources of the attack
- The applications to which the attack applies
- The notification and response actions associated with the attack signature.

Custom attack signatures were designed to detect specific attacks targeted towards specific operating systems or applications. (Each custom attack signature is associated with a type of application and operating system. Thus, when the Profiler detects an application running on a detected system, it can suggest all the attack signatures associated with that application. For example, if the Profiler discovers a system running HTTP server software, it can suggest the activation of the *Apache Web Server Denial of Service* attack signature, the *HTTP ETC Password Decode* attack signature, and other HTTP-related attack signatures.

Appendix C: Attack Signature Descriptions lists the majority of these attack signatures and the types of operating systems they were designed to be associated with.

User-defined Attack Signatures

NetProwler allows you to create and activate your own attack signatures. Once you have created them, you can activate and deactivate them in the same way that you do the custom attack signatures.

For information and instructions on how to create your own attack signatures, see *Chapter 7: Creating Attack Signatures.*

Modifying Common Attack Signatures

Some of NetProwler's Common attack signatures use threshold settings that you can modify. This section describes how to adjust those settings. Adjusting settings periodically can help deter experienced hackers who look for defined thresholds and ways to circumvent them

Adjusting the Port Scan Threshold

By default, NetProwler logs an alarm when 20 ports have been scanned on the same system within 60 seconds. The following instructions describe how to adjust this threshold.

To adjust the Port Scan threshold:

1. In the **Configure** tree, expand the **Attacks** branch, and select **Port Scan**.

   The following Port Scan configuration fields should be visible.

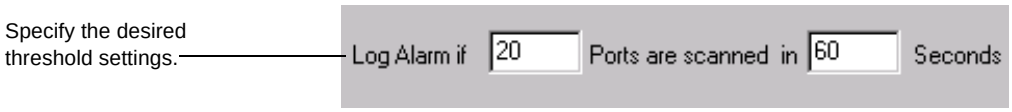


Figure 6-3: Port Scan Threshold Settings

2. Specify the desired threshold settings.

Specify the time in seconds.

3. When finished, click **Apply** to save the changes.

   The Port Scan threshold settings are changed.

Adjusting the SYN Flood Threshold

By default, NetProwler will log an alarm when it detects eight half-open communication attempts and attempt to reset the same number, so as to prevent denial of service. The following instructions describe how to adjust these settings.

To adjust the SYN Flood threshold:

1. In the **Configure** tree, expand the **Attacks** branch, and then select **SYN Flood**.

   The following SYN Flood configuration fields should be visible.

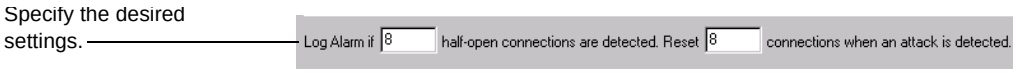

Specify the desired settings.
Log Alarm if 8 half-open connections are detected. Reset 8 connections when an attack is detected.

Figure 6-4: SYN Flood Threshold Settings

2. Specify the desired threshold and reset settings.
3. When finished, click **Apply** to save the changes.

   The Port Scan threshold settings are changed.

Adjusting the Denial of Service Threshold

By default, NetProwler logs a Denial of Service alarm when five ICMP Echo (ping) requests have been detected on the same system within 15 seconds. The following instructions describe how to adjust this threshold.

To adjust the Denial of Service threshold:

1. In the **Configure** tree, expand the **Attacks** branch, and select **Denial of Service**.

   The following Denial of Service configuration fields should be visible.

Figure 6-5: Denial of Service Threshold Settings

2. Specify the desired threshold settings.

   Specify the time in seconds.

3. When finished, click **Apply** to save the changes.

   The Denial of Service threshold settings are changed.

Adjusting the TCP/IP Spoofing Settings

A key part of the TCP/IP Spoofing attack occurs when an external source impersonates a trusted internal source. NetProwler detects the attack by comparing the expected MAC address with actual MAC address. If they are different, then NetProwler logs the alarm. Therefore, when configuring NetProwler to monitor a host for a TCP/IP Spoofing attack, you must tell NetProwler where the remote system resides on the network in relation to where NetProwler is installed. Otherwise, you may experience some false positive alarms. You must tell NetProwler if the remote system is "Internal" meaning on the same subnet as NetProwler, "Router," meaning the system is a router, or "External," meaning that there is at least one router between the remote system and NetProwler.

In addition, you can configure this attack signature to detect spoofed TCP sequence numbers. Spoofed sequence numbers fall outside the expected boundaries. Attackers have at their disposal the ability to calculate and fairly accurately guess the TCP sequence number; however, their guess may be off. NetProwler can detect and respond to these attempts.

The following instructions describe how to configure the TCP/IP Spoofing attack signature.

To adjust the TCP/IP Spoofing settings:

1. In the **Configure** tree, expand the **Attacks** branch, and then select **TCP/IP Spoofing**.
2. Click **Add New**.

   The TCP/IP Spoofing dialog box appears.

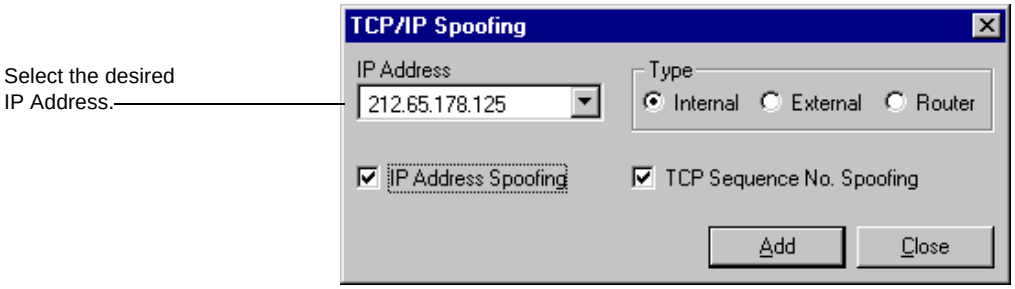


Figure 6-6: TCP/IP Spoofing Dialog Box

3. In the **IP Address** drop-down list, select the desired system.
4. In the **Type** box, select the desired type.

   Each type is discussed in the following table.

Type	Description
Internal	If the selected host resides on the same subnet as NetProwler, select this option.
External	If one or more routers fall between the remote host and NetProwler, select this option.
Router	If the remote host is a router, select this option.

Table 6-1: TCP/IP Spoofing Types

5. To enable IP address spoofing, check the **IP Address Spoofing** check box.

   Or

   To disable IP address spoofing, leave the **IP Address Spoofing** check box unchecked.

6. To enable the monitoring of TCP sequence number spoofing, check the **TCP Sequence No. Spoofing** check box.

   Or

   To disable the monitoring of TCP sequence number spoofing, leave the **TCP Sequence No. Spoofing** check box unchecked.

7. Click **Add**.
8. Repeat **Steps 3–7** for additional hosts.
9. When finished adding systems, click **Close**.
10. Click **Apply** to save the changes.

    The TCP / IP Spoofing settings are modified.

Adjusting the Ping of Death Settings

To adjust the Ping of Death threshold settings:

1. In the **Configure** tree, expand the **Attacks** branch, and select **Ping Of Death**.

   The following Ping of Death configuration fields should be visible.

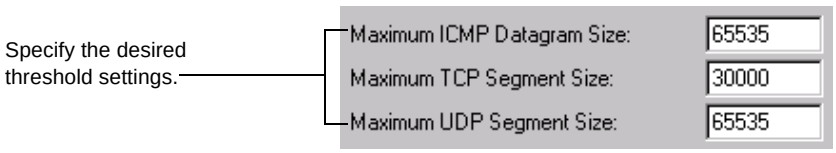


Figure 6-7: Port Scan Threshold Settings

2. In the **Maximum ICMP Datagram Size** field, specify maximum size of the ICMP datagram.
3. In the **Maximum TCP Segment Size** field, specify maximum size of the TCP segment.
4. In the **Maximum UDP Segment Size** field, specify maximum size of the UDP segment.
5. When finished, click **Apply** to save the changes.

   The Ping of Death threshold settings are changed.

Associating Attack Signatures Manually

NetProwler begins monitoring a system for selected attacks, once those attacks are "associated" with that system. Attack signatures are not activated on the system; they do not reside on the system. Rather, NetProwler monitors the network for traffic going to and from a configured system. If the traffic to that system matches the attack signature criteria, then NetProwler logs an alarm and any other configured actions.

There are two methods of associating attack signatures with a host: using the Profiler and manually. The instructions in this section describe how to manually associate an attack signature with a selected host. For instruction on how to run the Profiler and automatically configure systems with attack signatures, see *Profiling a Network* on page 5.2.

Before being able to associate an attack signature with a system, the system must reside in the NetProwler Address Book. For instruction on how to manually enter systems in the NetProwler Address Book see *Adding Systems to the Address Book Manually* on page 5.16.

To manually associate attack signatures:

1. In the **Configure** tree, expand the **Custom Attacks** branch, and then select **Attack Association**.

   The list of configured systems should be visible.

2. Right-click on the desired system in the list, and then choose Modify.

   The Edit Attack Association dialog box appears.

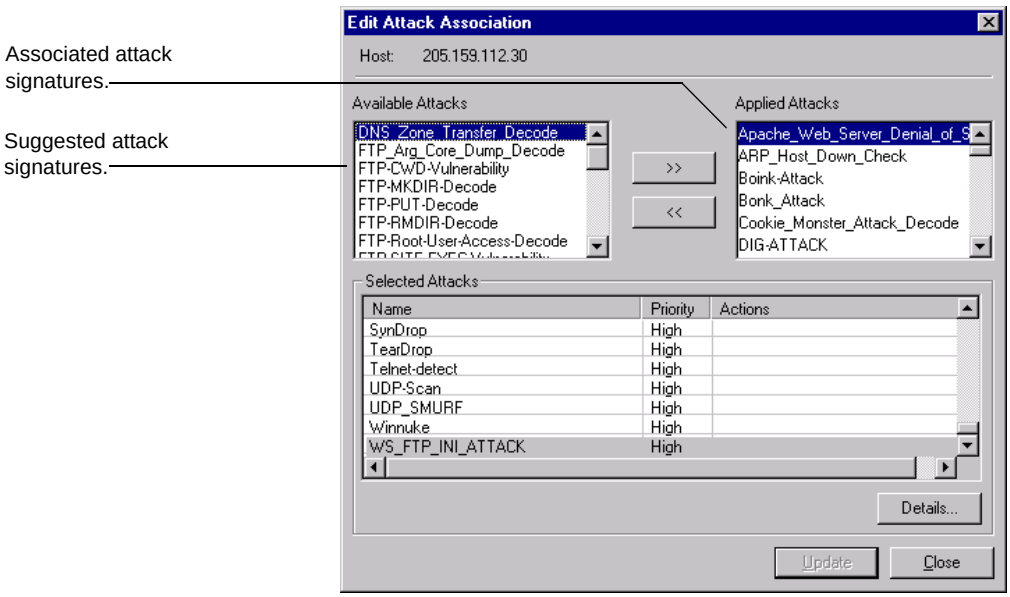


Figure 6-8: Edit Attack Association Dialog Box

NetProwler suggests a list of attack signatures to activate based on the type of operating system.

3. Associate attack signatures by selecting them in the **Available Attacks** box and then clicking the **Right Arrow** button.

4. Remove an applied attack signature by selecting it in the **Applied Attacks** box and then clicking the **Left Arrow** button.

5. (Optional) To modify an attack signature, select the desired attack signature in the **Selected Attacks** box, and then click **Details**.

The Edit Attack Association Details dialog box appears.

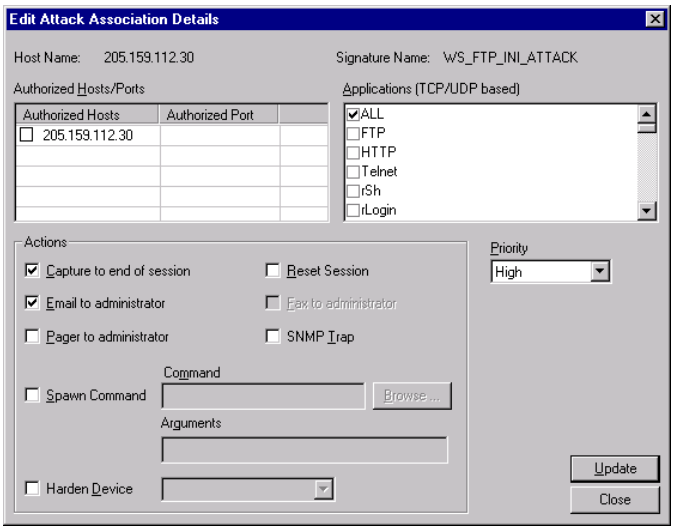


Figure 6-9: Edit Attack Association Details

6. Select the desired options.

   The following table describes each option.

To	Do This
Allow authorized users access to a monitored resource without NetProwler reporting an attack. Also lets you designate a port or ports that the user must use.	Locate the host in the Authorized box and check its check box. (If the attack stems from an authorized source, no alarm or response will trigger.)
Configure which applications are associated with this attack	In the Applications box, check the associated applications.

Table 6-2: Modification Options

To	Do This
Select which action mechanisms to trigger when an attack is detected	Check the desired notification and response actions in the Action box. (NetProwler must also be set up with the capabilities to send e-mail, page, send SNMP traps, and harden a firewall.)
Change the attack signature's priority level	Select the desired priority (High, Medium, or Low) in the Priority drop-down list box.

Table 6-2: Modification Options

7. When finished modifying the attack signature, click **Update**.
8. After making the desired configuration changes, click Update.

   The Edit Attack Association box reappears.
9. Click **Update**.
10. To save and activate the changes, click **Apply**.

    The attack signatures are associated with the configured system. NetProwler begins immediately monitoring the configured systems for their associated attacks.

Disassociating an Attack Signature

After you have configured a system to detect a list of selected attacks, you can remove an attack signature from this list. The following instructions describe how to remove or disassociate an attack signature from a system.

To disassociate an attack signature:

1. In the **Configure** tree, expand the **Custom Attacks** branch, and then select **Attack Association**.

   The list of systems should be visible in the Configure pane.

2. Right-click on the desired system, and select **Modify**.

   The Edit Attack Association dialog box appears.

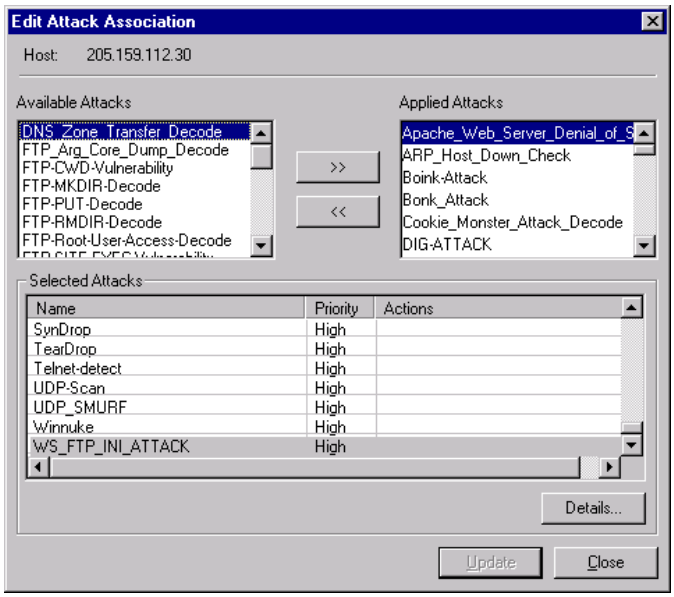


Figure 6-10: Edit Attack Association Dialog Box

3. Remove an applied attack signature by selecting it in the **Applied Attacks** box and then clicking the **Left Arrow** button.

4. After making the desired configuration changes, click **Update**.

   The list of associated attacks is updated.

5. To save and activate the changes, click **Apply**.

NetProwler begins immediately monitoring the configured systems for their associated attacks.

Deleting an Attack Signature

After you have created or imported an attack signature into NetProwler you can delete it.

You cannot delete any of NetProwler's preconfigured attack signatures.

To delete an attack signature from NetProwler:

1. In the **Configure** tree, expand the **Custom Attacks** and **Attack Definition** branches.

   The list of attack signatures should be visible.

2. Select the desired attack signature in the list, and then click **Delete**.

   The selected attack signature is deleted from the system.

Changing an Attack Signature's Priority Level

Out of the box, NetProwler comes with a number of predefined attack signatures. All of these attack signatures are assigned the default priority level: High. To change the priority level, NetProwler requires that you change it by attack signature and host. This means that the same attack signature can have a different priority level on different systems.

You can change the priority level of an attack signature during the process of profiling the network. However, the instructions contained in this section describe how to manually change it after a system has already been configured with attack signatures.

To change an attack signature's priority level:

1. In the **Configure** tree, expand the **Custom Attacks** branch, and then select **Attack Association**.

   The list of systems appear in the Configure pane.

2. Right-click on the desired system, and then choose **Modify**.

   The Edit Attack Association dialog appears.

3. In the **Selected Attacks** box, select the desired attack signature.

   The Priority drop-down list box becomes active.

4. Select the desired priority level.

5. Repeat **Steps 3–4** for additional attack signatures.

6. When finished, click **Update**.

7. In the **Configure** pane, click **Apply** to save the configuration changes.

   The new priority levels are applied.

Configuring NetProwler Actions

When configuring NetProwler's actions, it is helpful to differentiate between "notification" actions and "response" actions. Notification actions notify an administrator (via e-mail or pager) or device (such as a firewall or SNMP Manager) that a security-related event occurred. Response actions take action in

response to some kind of attack, such as capture the attacker's session, reset the session, or spawn a command. The following table describes NetProwler's notification actions.

Notification Action	Description
Send E-mail	NetProwler sends an email message to an email recipient.
Page an Administrator	Using a configured modem, NetProwler dials a paging service and pages an administrator.
Send an SNMP Trap	NetProwler acts as an SNMP Agent. When an attack occurs, NetProwler sends an SNMP trap to up to two SNMP Managers. The Manager must be configured to act on the trap received from NetProwler.
Harden a Firewall	NetProwler sends a Suspicious Activity Monitoring Protocol (SAMP) message to a configured firewall. The firewall must be configured to act on the SAMP notification message.

Table 6-3: Notification Actions

This next table describes NetProwler's response actions.

Response Action	Description
Reset Session	NetProwler terminates the session-based attack.

Table 6-4: Response Actions

Response Action	Description
Capture the Session	Upon detecting the attack, NetProwler records the remainder of the session. If you installed NetProwler in the default location, the session is stored in the <*Drive Letter*>:\Program Files\NetProwler\CapturedFiles folder.
Spawn a Command	NetProwler executes a specified command or batch file.

Table 6-4: Response Actions

In NetProwler, you can configure actions by priority level and by associated attack signature. Notification actions can be configured at both the priority level and attack signature level; however, only response action can be configured by attack signature, as illustrated in the following table.

	Priority Level	Associated Attack Signature
Notification Actions	Available	Available
Response Actions	Not Available	Available

Table 6-5: Configuration Options

To configure notification actions by priority level, see *Configuring Notification Actions by Priority Level* on page 6.22.

To configure response actions by attack signature, see *Configuring Response Actions by Attack Signature* on page 6.24

Configuring Notification Actions by Priority Level

NetProwler allows you to define notification actions by individual attack signature and by priority level. However, configuring actions for individual attacks can be time consuming. An easier and less time consuming approach is to configure notification responses by priority level. NetProwler offers three priority levels: High, Medium, and Low. The following table describes each level.

Priority Level	Description
High (Red)	High priority attacks are attacks that pose a serious security threat to the organization. Immediate action should be taken to stop any damage or prevent further damage from happening.
Medium (Blue)	Medium priority attacks are attacks that pose a moderate security threat to your organization. They do not require immediate attention.
Low (Yellow)	Low priority attacks are attacks that pose a minor threat to your organization. Corrective action may not be possible or is not required.

Table 6-6: Priority Levels Defined

For example, you can configure NetProwler so that all High priority attacks page an administrator.

Out of the box, all attack signatures are assigned a High priority level. For instructions on how to change an attack signature's priority level, see *Changing an Attack Signature's Priority Level* on page 6.18.

NOTE

NetProwler allows you to configure response actions by both priority level and associated attack signature. If an attack signature's notification actions differ from those configured by priority level, then the actions configured by attack signature take precedence.

To configure responses by priority level:

1. If you have not already set up NetProwler with the desired notification capabilities, do so before continuing.

   For instructions on setting up NetProwler to interface with the desired notification devices, see *Setting Up NetProwler's Notification Capabilities* on page 4.7.

2. In the **Configure** tree, expand the **Notification Options** branch, and then select **Associate Priorities**.

   The High, Medium, and Low Priority Actions configuration boxes appear.

Check the desired response mechanisms for each priority.

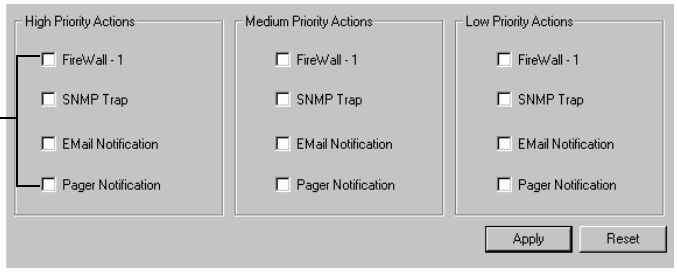


Figure 6-11: The Priority Configuration Boxes

3. Check the desired responses for each priority level.
4. Checked actions will be taken when attacks having that priority level are detected.
5. When finished, click **Apply** to save and apply the configuration changes.

NetProwler's notification actions are configured by priority level.

Configuring Response Actions by Attack Signature

As indicated in *Table 6-5: Configuration Options* on page 6.21, both notification and response mechanisms can be configured by associated attack signature. NetProwler allows you to configure the following actions in response to an attack.

- Capture to end of session
- E-mail an administrator
- Page an administrator
- Reset the session
- Send an SNMP trap
- Spawn a command
- Harden a firewall

The following instructions describe how to configure an associated attack signature with these responses. (Remember that an associated attack signature is an attack signature associated with a particular host.)

To configure response actions by attack signature:

1. In the **Configure** tree, expand the **Custom Attacks** branch, and then click **Attack Association**.

   The list of configured systems should be visible.

2. Right-click on the desired system in the list, and then choose **Modify**.

   The Edit Attack Association dialog box appears

3. Select the desired attack signature in the **Selected Attacks** box, and then click **Details**.

The Edit Attack Association Details dialog box appears.

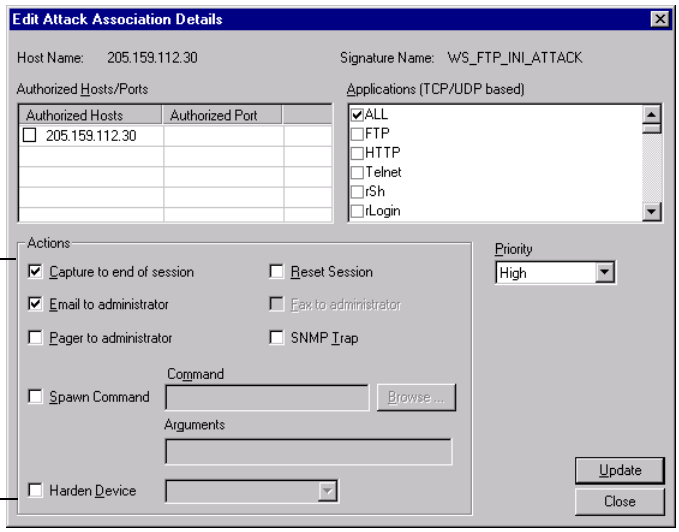


Figure 6-12: Edit Attack Association Details Dialog Box

4. In the **Actions** box, check and, where required, configure the desired actions.
5. After configuring the desired actions, click **Update**.

   The Edit Attack Association box reappears.
6. Click **Update**.
7. In the Configure pane, click Apply to save and activate the changes.

   The actions are configured. NetProwler immediately begins monitoring the configured systems for their associated attacks.

Creating Attack Signatures

Overview

NetProwler, unlike any network-based intrusion detection system on the market today, empowers customers with the ability to create their own attack signatures without requiring programming. Creating user-defined attack signatures is performed using NetProwler's Attack Signature Definition (ASD) toolkit.

In this chapter, you will learn:

- The attack signature development process
- How to use the ASD to create new attack signatures
- How to use the ASD Wizard

In addition, at the end of this chapter, you will find three tutorials that allow you to practice creating new attack signatures on your own.

As you begin, please note that creating attack signatures often requires a solid understanding of the protocols and applications used by an attacker. For example, to accurately determine the nature of a particular client/server command in a custom application, it is necessary to know how that command is communicated over the network, including the hexadecimal or ASCII command itself and the offset (location) at which the command occurs in a session. An excellent source of information about TCP/IP protocols is W. Richard Stevens' *TCP/IP Illustrated Volume 1: The Protocols*.

The Attack Signature Development Process

This section describes the steps for creating attack signatures in NetProwler.

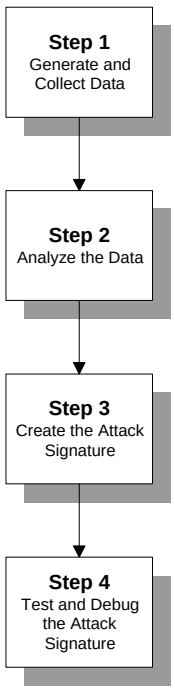


Figure 7-1: Attack Signature Development Process

Generate and Collect Data

In the generate and collect data phase, collect as much information about the attack as you can, including having some idea about the nature of that attack. Attacks can be categorized into one of two areas: connection-based (TCP) and nonconnection-based (UDP and ICMP). Knowing the type of the attack dictates how you will go about collecting events.

A connection-based attack uses the TCP protocol to establish or attempt to establish a connection with a remote system. An example of a connection-based attack is a port scan attack. (A port scan attack establishes a connection with a remote system and then seeks to establish connections with open and available ports on that system.) To detect connection-based attacks, you can configure NetProwler to record or capture the session. If you can capture the session, then you can analyze it contents at a later time.

Nonconnection-based attacks use UDP or ICMP protocols to carry out an attack. These protocols do not require an established connection and are often carried out in a single packet. NetProwler does not have a method of capturing these types of events; therefore, you must know enough about the protocol used in the attack to know where in the packet the attack is located. An example of a nonconnection-based attack is the Ping of Death attack. (The Ping of Death occurs when an oversized ICMP Echo Request command is sent to a remote host.) To create an attack signature to detect this attack, you must know where in the ICMP header the size is specified.

Moreover, if you can duplicate the attack, it will be easier to gather the data you need to effectively create and test the attack signature.

Analyze the Data

During this phase, you should identify all of the relevant information needed to create the attack signature. If you captured a session in NetProwler, the events of the session are stored in an ASCII text file. Open this file and begin analyzing what events constitute the attack. The following questions will help you get started:

- What events were generated by your actions?
- What protocol (s) were used in the attack?
- When did the events occur in relation to each other? (The sequence may be an important part of the attack.)
- On what type of system did the attack occur?
- What applications / ports were used in the attack?

These and many other questions need to be answered during the analysis phase. The object is to sort through all the information you have and determine what unique elements constitute the attack. This information is used to build the attack signature's selection criteria.

Create the Attack Signature

Now that you have analyzed the events and identified what elements constitute the attack, begin creating the attack signature in NetProwler. In order to effectively create an attack signature in NetProwler, you should be familiar with NetProwler's Attack Signature Definition toolkit, including the types of attack signatures and how Search Primitives, Value Primitives, Reserved Keywords and expressions are used to create attack signatures. For help in learning about the Attack Signature Definition tool, see *Understanding the Attack Signature Definition Tool* on page 7.5.

Test and Debug the Attack Signature

After creating the attack signature, associate it with a target system, and then run the attack against that system. Make sure to perform the same actions used in the data collection phase. Verify that NetProwler was able to detect and report the attack. Resolve any problems that might arise.

Understanding the Attack Signature Definition Tool

The Attack Signature Definition (ASD) toolkit provides you with the ability to create your own attack signatures. (The Attack Signature Definition tool is accessed from the Configure tree by choosing Custom Attacks, Attack Definition, and then Add New.)

This section is designed to teach you the components of the ASD and how to use those components to create new attack signatures. Before continuing, please familiarize yourself with

the components of the Attack Signature Definition dialog box. The following graphic illustrates the General tab. (The Expressions tab is illustrated on the following page.)

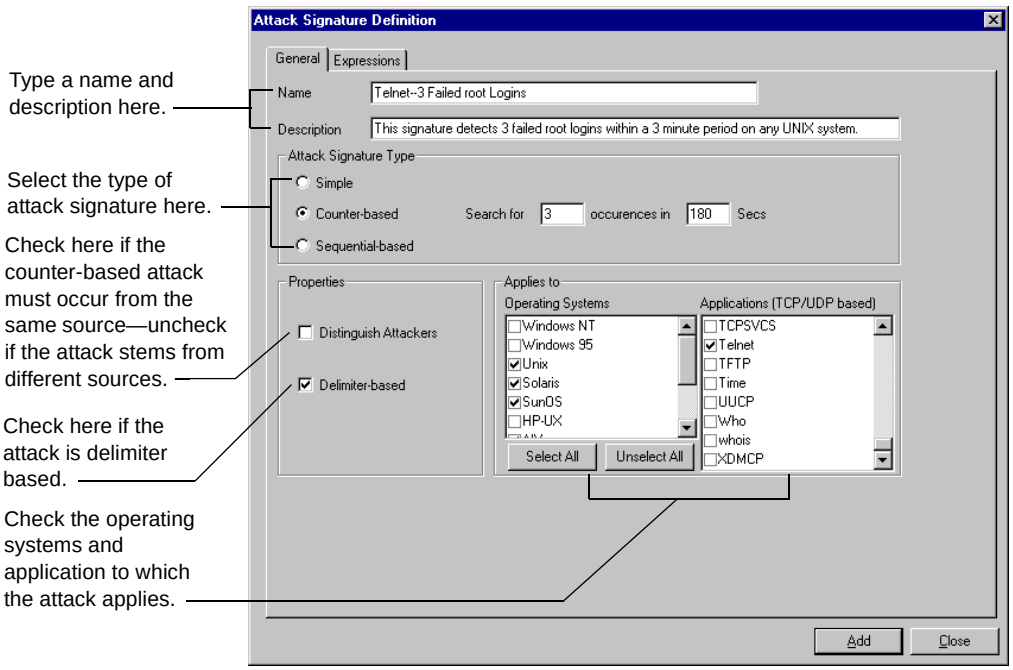


Figure 7-2: Attack Signature Definition Dialog Box (General Tab)

This next graphic illustrates the components of the Expressions tab.

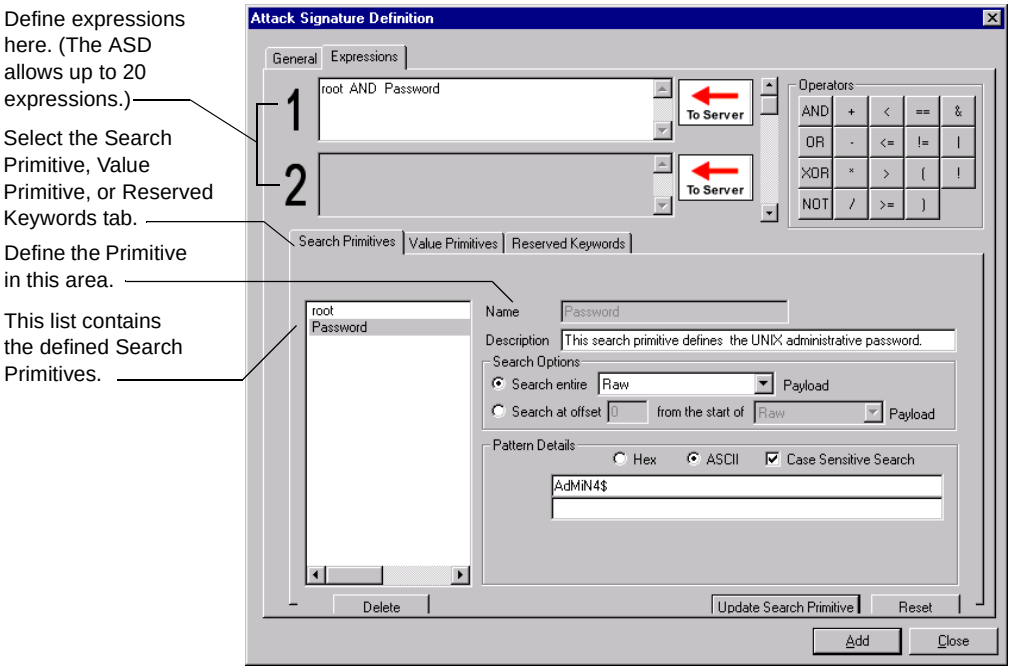


Figure 7-3: Attack Signature Definition Dialog Box (Expression Tab)

Each option in the General and Expressions tab are discussed in the following sections.

The General Tab

The General tab is used to define important elements of the attack signature, including the:

- Name
- Description
- Type of attack signature
- Properties
- Applicable operating systems and applications

Name and Description

The Name field defines the name of the attack signature. Be as brief and descriptive as possible. Multi-word names with spaces are allowed. The Description field allows you to enter a longer more detailed description of the attack signature (See Figure 7-2). In the description, it is helpful to list the applicable operating systems and/or applications to which the attack signature will apply. For example:

> *This attack signature detects 3 failed telnet logins on UNIX systems within a 1 minute period.*

Attack Signature Types

Custom attack signatures are grouped into one of three types: Simple, Counter-based, and Sequential-based. The following table describes each type and provides information about how to configure it.

Type	Description
Simple	A "simple" attack signature uses a single expression to detect the target attack. This expression may contain a single search primitive, value primitive, or reserved keyword only or a combination of search primitives, value primitives, and reserved keywords that form a logical statement. For more information on how to combine search primitives, value primitives, and reserved key words into logical statements, see *Building Expressions* on page 7.28. Select this option when the attack is comprised of a single network frame or session. NetProwler will search individual frames for matches to the defined search criteria.

Table 7-1: Attack Signature Types

Type	Description
Counter-based	A "counter-based" attack signature detects an attack that occurs repetitively within a given period of time. Each occurrence is counted by NetProwler. When the defined threshold is met, the attack is identified. This type of attack also uses a single expression to detect the target attack. This expression may contain a single search primitive, value primitive, or reserved keyword only or a combination of search primitives, value primitives, and reserved keywords that form a logical statement. For more information on how to combine search primitives, value primitives, and reserved key words into logical statements, see *Building Expressions* on page 7.28. To configure this option, specify how many times the event must occur within a given amount of time. Specify the time in seconds. An example is an attack signature that detects three failed administrative logins within 60 seconds. Select this option when the attack is comprised of multiple occurrences of the same event.

Table 7-1: Attack Signature Types

Type	Description
Sequential-based	A "sequential-based" attack signature detects an attack that occurs in two to twenty parts. These parts may be comprised of multiple frames using multiple applications. For example, network probes often consist of multiple parts, such as attempts to logon using telnet, rlogin, finger, and others. The sequential-based attack signature would then attempt to detect enough of these components to positively identify the attack. This type of attack signature uses multiple search primitives, value primitives, reserved keywords, or expressions to identify an attack. Select this option when the attack consists of multiple parts and requires multiple expressions to detect the attack.

Table 7-1: Attack Signature Types

Attack Signature Properties

There are two attack signature properties:

- Distinguish Attackers
- Delimiter-based

The following table describes each option and when to use it.

Property	Description
Distinguish Attackers	This option is available with both Counter-based and Sequential-based attack signatures. When checked, it requires that the threshold specified in the *Search for* box be met by the same host. Leaving it unchecked means that the threshold can be satisfied by any hosts. For example, four failed logins from four remote hosts within a two minute period may be normal; however, four failed logins from the same remote host within a two minute period may be indicative of an attacker attempting to gain access to the system. Check this option when you want the threshold to be met by a single host. Uncheck this option when any combination of hosts satisfies the threshold.

Property	Description
Delimiter-based	Delimiter-based means that the content of the network frame is delimited in some way. Certain applications such as telnet, rLogin, and rSH send data across the wire in some kind of delimited format. Check this option if the information you want to detect is delimited in some way.

Table 7-2: Description of Properties

Applicable Operating Systems and Applications

In the Applies to box, you can select the operating systems and applications to which the user-defined attack signature applies. NetProwler uses this information when suggesting attack signatures to associate with a profiled or manually configured system.

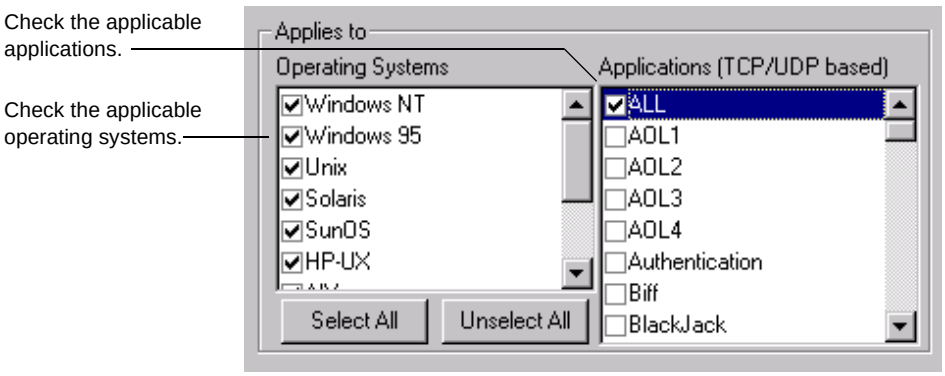


Figure 7-4: Applies To Box

If the attack signature is operating system independent, check the Select All button. If the attack signature applies to only selected operating systems, check the applicable systems.

Similarly, if the attack signature applies to all applications configured in the Application Book, check the All check box. If the attack signature applies to only selected applications, check the applicable applications.

The Expressions Tab

The Expressions tab is used to define the attack signature's search criteria. The search criteria will be composed of Search Primitives, Value Primitives, and Reserved Keywords.

Search Primitives

A search primitive defines an ASCII or hexadecimal pattern to search for and where to locate that information in an Ethernet frame. A search primitive may be used alone or as part of an expression. For more information about how to use search primitives to create expressions, see *Building Expressions* on page 7.28.

The following graphic illustrates the Search Primitives tab.

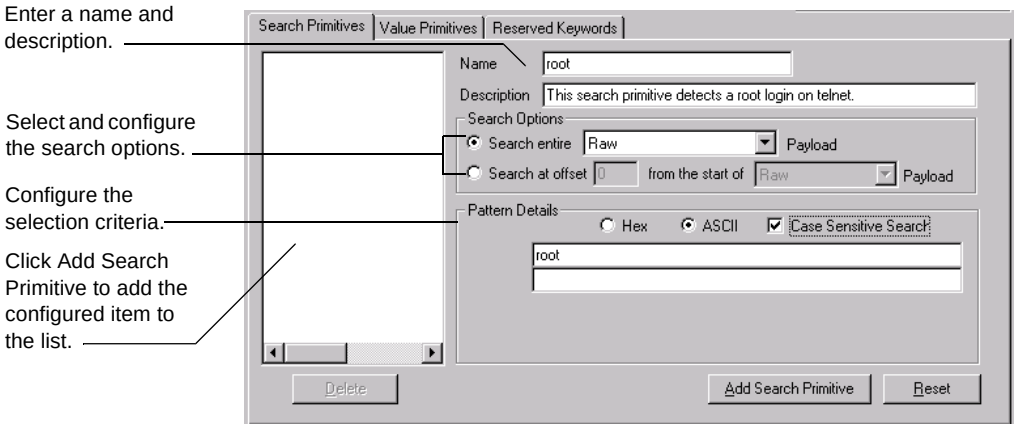


Figure 7-5: Search Primitives Tab

The following table defines each option on the Search Primitive tab and describes how to configure it.

Item	Description
Name	The name of the search primitive. Type the name of the primitive. **Note:** Because the primitive may be used within expressions, the name cannot contain spaces.
Description	The description of the search primitive. Entering a description is optional.
Search Entire __ Payload	An option telling NetProwler what part of the network frame to search. Options include: Raw, MAC, Network (IP), and Transport (TCP or UDP). **Raw** refers to the entire frame. **MAC** refers to from where the MAC header begins to the end of the packet. **Network** refers to from where the IP header begins to the end of the packet. **Transport** refers to from where the TCP or UDP header begins to the end of the packet.
Search at offset __ from the start of __ payload	A option telling NetProwler where to begin searching in the network frame. The offset refers to where in the packet the data resides. Specify the offset in bytes, and then configure the search criteria in the Pattern Details box.

Table 7-3: Search Primitive Options

Item	Description
Hex radio button	Directs NetProwler to use the hexadecimal value system when searching frames for the search criteria. When checked, NetProwler searches for hexadecimal values instead of ASCII text. In the Offset fields, type the hexadecimal values in the location where they are found in the frame.
ASCII radio button	Directs NetProwler to use the ASCII character code when searching frames for the search criteria.
Case Sensitive Search	An option that directs NetProwler to differentiate between upper and lower case letters. This option is associated with the ASCII option only.
Add Search Primitive button	Adds the search primitive to the list of available search primitives. Search primitives are added to an expression by dragging them from the search primitive list and dropping them in the Expression box.
Reset button	Clears all entries in the Search Primitive tab.

Table 7-3: Search Primitive Options

Value Primitives

Value primitives define a particular part of a packet that can be extracted from a session and then evaluated. Value primitives allow you to monitor a value in a network frame and ensure that it lies within the expected range of values. A value primitive may be used alone or within an expression.

The following graphic illustrates the Value Primitives tab.

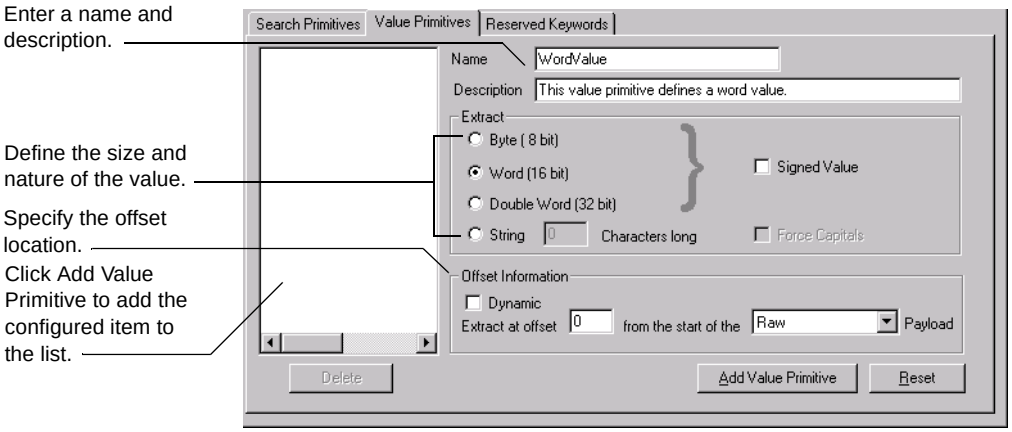


Figure 7-6: Value Primitives Tab

The following table defines each option on the Value Primitives tab.

Item	Description
Name	The name of the value primitive. Type the name of the primitive in this field. **Note:** Because the name is used within expressions, the name cannot contain spaces.
Description	The description of the value primitive. Entering a description is optional.

Table 7-4: Value Primitive Options

Item	Description
Byte (8 bit)	The size of value equivalent to 8 bits.
Word (16 bit)	The size of value equivalent to 16 bits.
Double Word (32 bit)	The size of value equivalent to 32 bits.
Signed Value	A method of comparing one value with another.
String __ Characters Long	A specified size of value. Enter the size of the value in bits.
Force Capitals	Forces NetProwler to evaluate the characters in capital letters. If the text is a mixed case string like "Admin," you can look for it as "ADMIN" and it will match. This prevents having a hacker avoid detection by saying AdMin or some another variant.
Dynamic	An option that tells NetProwler where to locate the defined value in the network frame. When checked, NetProwler will search the entire frame for the specified value, regardless of its offset. If the protocol you are searching uses fixed length fields, leave this option unchecked and define the offset location. If the protocol you are searching uses variable length fields, check this box. When checked, you have the option of defining an offset parameter as an argument in an expression. The argument must be a numeric value. The numeric argument can be a numeric value, search primitive defining a numeric value, value primitive returning a numeric value, or arithmetic expression.

Table 7-4: Value Primitive Options

Item	Description
Extract at offset __ from the start of __ Payload	A option telling NetProwler where to begin searching in the network frame. Options include: Raw, MAC, Network (IP), and Transport (TCP or UDP). **Raw** refers to the entire frame. **MAC** refers to from where the MAC header begins to the end of the packet. **Network** refers to from where the IP header begins to the end of the packet. **Transport** refers to from where the TCP or UDP header begins to the end of the packet. The offset refers to where in the packet the data resides. Specify the offset in bits.
Add Value Primitive button	After defining the value primitive, click this button to add it to the list of available value primitives. Value primitives are added to an expression by dragging them from the value primitive list and dropping them in the Expression box.
Reset button	Clears all entries in the Value Primitive tab.

Table 7-4: Value Primitive Options

Reserved Keywords

Reserved keywords are predefined search elements. Reserved keywords can be classified into two categories:

- True / False (T / F)
- Numeric (#)

True / false reserved keywords are either the selected keyword or they are not. For example the reserved keyword “TCP” is a true / false data type because the packet is either TCP or it is not. Numeric reserved keywords identify a numeric value. For example, the reserved keyword IP_SRC_ADDRESS is used in an

expression to identify the IP source address, such as: IP_SRC_ADDRESS == 199.78.122.1 or IP_SRC_ADDRESS == IP_DEST_ADDRESS.

The following graphic illustrates the Reserved Keywords tab. These keywords are configured by dragging them from the Reserved Keywords box and dropping them in the desired location in an expression.

Drag and drop these keywords into the desired expression.

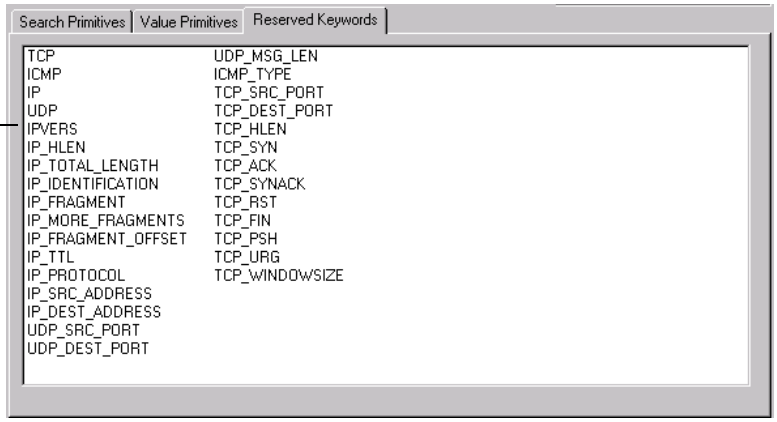


Figure 7-7: Reserved Keywords Tab

The following tables define each reserved keyword.

Protocol Names	Type	Description
TCP	T/F	Is this a TCP segment?
ICMP	T/F	Is this an ICMP packet?
IP	T/F	Is this an IP datagram?
UDP	T/F	Is this an UDP datagram?

Table 7-5: Reserved Keywords—Protocols

IP Header Parameters	Type	Description
IPVERS	#	The version of TCP / IP used. (4 bits [0-4])
IP_HLEN	#	The size (length) of the IP header. (4 bits [4–7])
IP_TOTAL_ LENGTH	#	The total length of the IP datagram in bytes. (16 bits [16–31])
IP_IDENTIFIC-ATION	#	The number that uniquely identifies each datagram sent by a host. (The identification number usually increments by one each time a datagram is sent.) (16 bits [32–47])
IP_FRAGMENT	T / F	Is the IP fragment flag set? (3-bits [48–50])
IP_MORE_ FRAGMENTS	T / F	Is the IP more fragment flag set? (3-bits [48–50])
IP_FRAGMENT _OFFSET	#	The value in the IP Fragment Offset position in bytes. (13-bits [51–63])
IP_TTL	#	The IP packet's time to live setting. The time to live setting refers to the number of routers through which the datagram can pass. The sender creates this value (often 32 or 64) and every time the datagram passes through a router, the number decrements by one. (8 bits [64–71])

Table 7-6: Reserved Keywords—IP Header

IP Header Parameters	Type	Description
IP_PROTOCOL	#	When a packet is received at the destination host, it starts up the protocol stack. This field identifies which protocol gave the data to IP to send. (8 bits [72–79])
IP_SRC_ ADDRESS	#	The IP datagram's source address. (32 bits [96–127])
IP_DEST_ ADDRESS	#	The IP datagram's destination address. (32 bits [128–159])

Table 7-6: Reserved Keywords—IP Header

ICMP Header Parameters	Type	Description
ICMP_TYPE	#	The ICMP message type. Message types include: 0 Echo Reply 3 Destination Unreachable 4 Source Quench 5 Redirect 6 Alternate Host Address 8 Echo Request 9 Router Advertisement 10 Router Solicitation 11 Time Exceeded 12 Parameter Problem 13 Timestamp Request 14 Timestamp Reply 15 Information Request 16 Information Reply 17 Address Mask Request 18 Address Mask Reply (located in the ICMP message header [8 bits 0–7])

Table 7-7: Reserved Keywords—ICMP Header

UDP Header Parameters	Type	Description
UDP_SRC_PORT	#	The UDP datagram's source port number. (16 bits [0–15])
UDP_DEST_ PORT	#	The UDP datagram's destination port number. (16 bits [16–31])
UDP_MSG_LEN	#	The length of the UDP header and UDP data in bytes. (16 bits [32–63])

Table 7-8: Reserved Keywords—UDP Header

TCP Header Parameters	Type	Description
TCP_SRC_PORT	#	The TCP segment's source port number. (16-bits [0–15])
TCP_DEST_ PORT	#	The TCP segment's destination port number. (16 bits [16–31])
TCP_HLEN	#	The size of the TCP segment's header. (4 bits [96–99])
TCP_URG	T/F	The urgent pointer is set. (1 bit [106])
TCP_ACK	T/F	The acknowledgment flag is set.(1 bit [107])
TCP_PSH	T/F	The push flag is set. (This flag tells the receiver to pass the data to the application as soon as possible.) (1 bit [108])

Table 7-9: Reserved Keywords—TCP Header

TCP Header Parameters	Type	Description
TCP_SYNACK	T/F	The SYN and the ACK flags are set, indicating the second segment in the three-way handshake.
TCP_RST	T/F	The reset flag is set. (The reset flag resets the connection.) (1 bit [109])
TCP_SYN	T/F	The synchronize sequence number is set. (The SYN flag is used to initiate a connection.) (1 bit [110])
TCP_FIN	T/F	The finish flag is set. (The finish flag tells the receiver that the sender is finished sending data.) (1 bit [111])
TCP_WINDOW SIZE	#	The size of the TCP window—the number of bytes the receiver is willing to accept. (16 bits [112–127])

Table 7-9: Reserved Keywords—TCP Header

Operators

NetProwler uses operators to combine search primitives, value primitives, and reserved keywords to create expressions.

The following table defines each operator.

Logical Operator	Description
AND	Both the preceding and following arguments must be true to satisfy the selection criteria. For example: X AND Y.
OR	Either the preceding or the following argument can be true to satisfy the selection criteria. For example: X OR Y.
XOR	The select criterion is met only when the preceding and the following arguments are different. For example: X XOR Y.
NOT	The select criterion is met when NetProwler finds anything but the specified value. For example: NOT X or X NOT Y.

Table 7-10: Logical Operators

Bit-wise Operator	Description
&	Bit-wise AND
|	Bit-wise OR
!	Bit-wise NOT

Table 7-11: Bit-wise Operators

Equality Operator	Description
>	Greater than
>=	Greater than or equal to
<	Less than
<=	Less than or equal to
==	Equal to (In computer science, a single equal sign (=) is used for assignment, and a double equals (==) is used for equals. NetProwler has adopted this standard to eliminate confusion.)
!=	Not equal to

Table 7-12: Equality Operators

Arithmetic Operator	Description
+	Add
-	Subtract
*	Multiply
/	Divide

Table 7-13: Arithmetic Operators

Combination Operator	Description
(	Beginning parenthesis. Indicates the start of an embedded expression. Parentheses allow you to create complex expressions, such as "(X OR Y) AND (A AND B)."
)	Ending parenthesis. Indicates the end of an embedded expression.

Table 7-14: Combination Operators

Building Expressions

NetProwler uses expressions to define attack signatures. Expressions identify the unique elements of an attack. They are created in the Expressions box (or boxes if you are creating a Sequential-based attack signature) on the Attack Signature Definition tool. Expressions may consist of:

- A single primitive or reserved keyword
- A simple expression
- A complex expression

Each option is discussed in the sections that follow.

Using Single Primitives or Reserved Keywords

Primitives and reserved keywords can be used individually to detect attacks. For example, you can define a search primitive that identifies the use of the root password on UNIX systems. With this single primitive in the Expressions box, NetProwler will search for use of the password in the configured TCP/IP traffic. When identified, NetProwler will report the attack and execute any configured response mechanisms.

Creating Simple Expressions

Simple expressions consist of two primitives or reserved keywords and one operator, as illustrated in the following graphic.

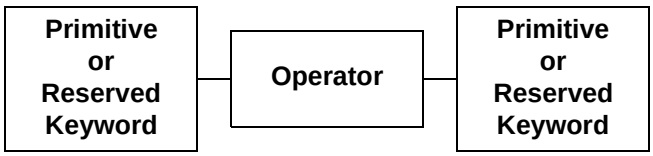


Figure 7-8: Form of Simple Expressions

Examples include:

IP_DEST_ADDRESS == IP_SRC_ADDRESS

Root AND Password

ICMP_TYPE == 5

Creating Complex Expressions

Simple expressions can be combined with single primitives, single reserved keywords, or other expressions to form complex expressions, as illustrated in the following figure.

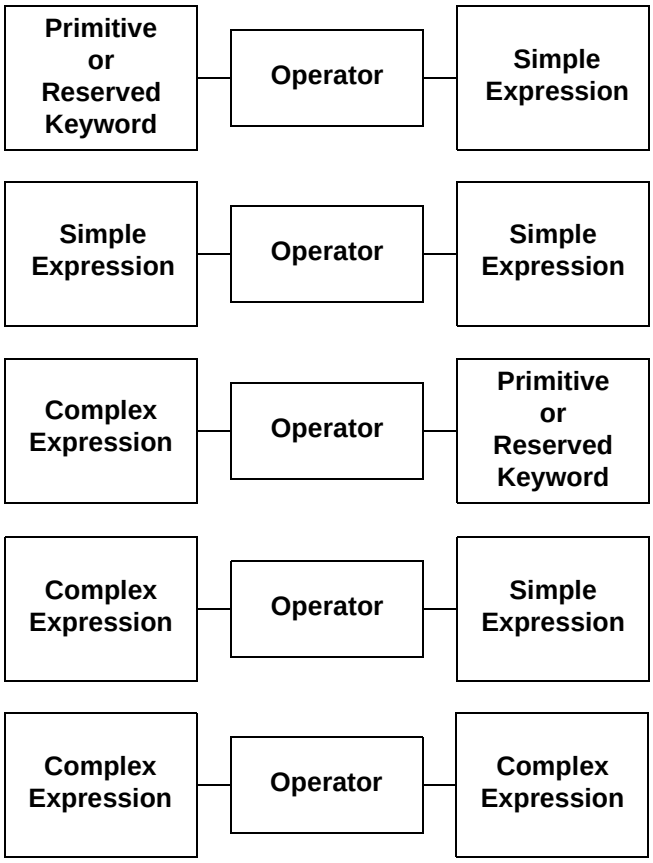


Figure 7-9: Forms of Complex Expressions

Complex expressions allow you to be very precise about the information you want to select. When combining expressions to create complex expressions, you must use parentheses to group expressions. The order of precedence is left to right, inside the parenthesis to outside.

The following are examples of complex expressions.

(Root AND Password) AND Access_ETC_Dir

(ICMP_TYPE == 5) AND ((IP_SRC_ADDRESS < 202.98.131.255) OR (IP_SRC_ADDRESS > 202.98.133.0))

((IP_SRC_ADDRESS == IP_DEST_ADDRESS) AND (IP_SRC_PORT == IP_DEST_PORT))

Setting the Network Frame Direction

You can select a frame based on the direction in which it is traveling. In the Expressions tab, the Direction button lets you choose to examine a packet traveling from the server, from the client, or either direction.

The **To Server** option selects a packet that matches the criteria defined in the adjacent expressions box and is going to the server (i.e. a remote client is sending a packet to the server.) NetProwler will ignore packets sent from the server, even if they match the expression's selection criteria.

The **To Client** option selects a packet that matches the criteria defined in the adjacent expressions box and is going to the client (i.e. the server is replying to the client. NetProwler will ignore packets sent from the client to the server, even if they match the expression's selection criteria.

The **Any** option selects a packet that matches the criteria defined in the adjacent expressions box and is going either direction. Choose this option when the direction of the packet is irrelevant.

Click the button until the desired direction appears.

Creating an Attack Signature

Before creating attack signatures in NetProwler, you should be familiar with the process for creating new attack signatures and the components of the Attack Signature Definition tool. To learn about the development process, please see *The Attack Signature Development Process* on page 7.2, and *Understanding the Attack Signature Definition Tool* on page 7.5.

To help you understand and practice the process of creating new attack signatures, AXENT has included three tutorials that walk you through the process of creating three actual attack signatures. Please refer to these tutorials in the section, *Attack Signature Tutorials* on page 7.39.

The following instructions describe the generic process for creating new attack signatures.

To create an attack signature:

1. In the **Configure** tree, expand the **Custom Attacks** and **Attack Definition** branch.

   The list of attack signatures should be visible.

2. Click **Add New**.

The Attack Signature Definition dialog box appears.

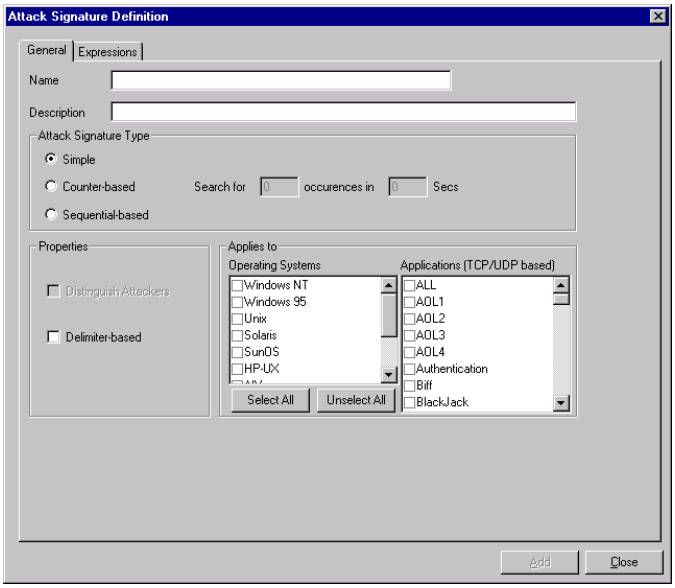


Figure 7-10: Attack Signature Definition Dialog Box

3. In the **Name** field, type the name of the attack signature.
4. (Optional) In the **Description** field, type a description.
5. In the **Attack Signature Type** box, select an attack signature type.

   Select Simple if only one expression is needed to detect the attack. Select Counter-based if only on expression is needed to detect an attack that occurs multiple times within a given period of time. Select Sequential-based two to twenty expressions are needed to detect the attack. For more information about each of these attack signature types, see *Attack Signature Types* on page 7.9.
6. (Optional) In the **Properties** box, select the desired property.

   If you selected Counter-based above, you can select the Distinguish Attackers check box to differentiate between attackers. If the attack's application sends information in

a delimited way, such as telnet, rLogin, and rSH, select Delimiter-based. For more information about each property, see *Attack Signature Properties* on page 7.12.

7. In the **Applies To** box, select the operating systems and applications to which this attack signature will apply.

   NetProwler uses this information when configuring systems with associated attack signatures.

8. Click the **Expressions** tab.

   The Expressions tab appears.

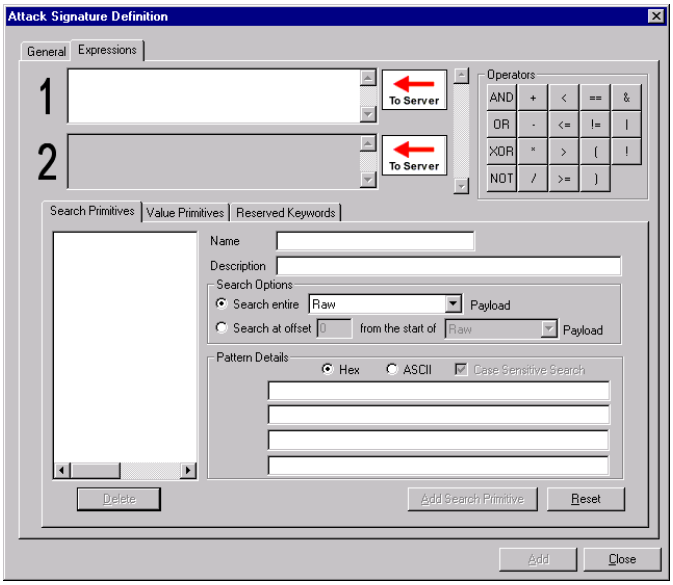


Figure 7-11: Expressions Tab

9. Configure the desired **Search Primitives**.

   For more information about how to create a Search Primitive, see *Search Primitives* on page 7.14.

10. Configure the desired **Value Primitives**.

11. Build the desired expressions using the configured search primitives, value primitives, reserved keywords and available operators.

For more information about how to build expressions, see *Building Expressions* on page 7.28.

12. When finished building the expressions, click **Add** to add the new attack signature to the list.
13. (Optional) Repeat **Steps 3–12** to create additional attack signatures.
14. When finished, click **Close**.
15. To save all changes, click **Apply**.

    The attack signature has been created. To become active, the attack signature must be associated with a configured host. For instructions on how to associate an attack signature with a host, see *Associating Attack Signatures Manually* on page 6.13.

Using the Attack Signature Definition Wizard

The Attack Signature Definition Wizard, or ASD Wizard, guides you through the process of creating simple attack signatures. (The ASD Wizard walks you through creating a single ASCII-based search primitives; value primitives and reserved keywords are not available in the ASD Wizard.) To create more sophisticated attack signatures, you must use the Attack Signature Definition tool. For more information about the Attack Signature Definition tool see *Understanding the Attack Signature Definition Tool* on page 7.5, and for instructions on how to create an attack signature using the Attack Signature Definition tool, see *Creating an Attack Signature* on page 7.32.

To create an attack signature using the ASD Wizard:

1. From the **Tools** menu, select **ASD Wizard**.

The Search Primitive Creation dialog box appears.

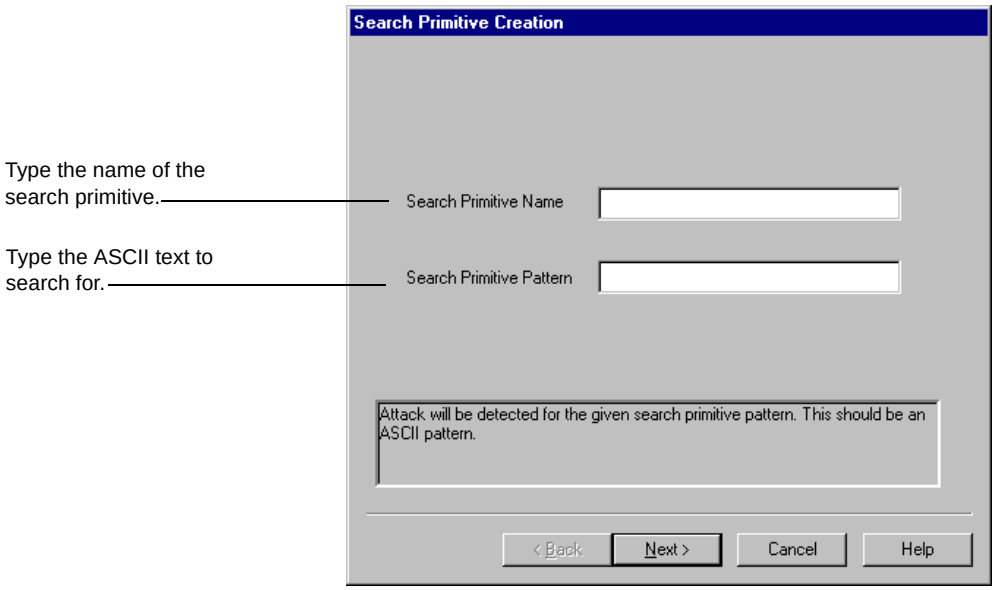

Type the name of the search primitive.
Type the ASCII text to search for.
Search Primitive Creation
Search Primitive Name
Search Primitive Pattern
Attack will be detected for the given search primitive pattern. This should be an ASCII pattern.
< Back
Next >
Cancel
Help

Figure 7-12: Search Primitive Creation Dialog Box

2. In the **Search Primitive Name** field, type the name of the new search primitive.

   This field names a new search primitive; it should not be used to specify an existing search primitive.

3. In the **Search Primitive Pattern** field, type the ASCII text that you want to search for.

   NetProwler will search the entire frame for the specified text.

4. Click **Next**.

The Attack Signature Template dialog box appears.

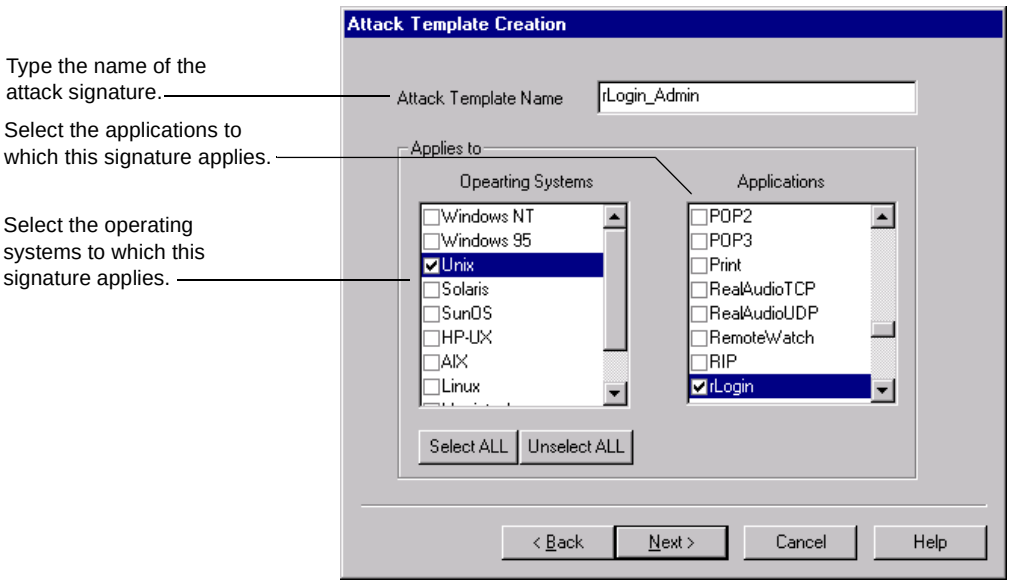


Figure 7-13: Attack Signature Template Dialog Box

5. In the **Attack Template Name** box, type the name of the attack signature.

6. In the **Applies To: Operating Systems** box, select the operating systems to which this attack signature will apply.

   NetProwler uses the operating system and application information to suggest hosts (configured in the Address Book) on which to activate this attack signature. (NetProwler lists these hosts in the next dialog. See Figure 7-14.)

   For example, if you select SunOS and Telnet, the ASD Wizard will list all SunOS systems in the Address Book configured with a Telnet server.

7. In the **Applies To: Applications** box, select the applications to which this attack signature will apply.

8. Click **Next**.

The Attack Association dialog box appears.

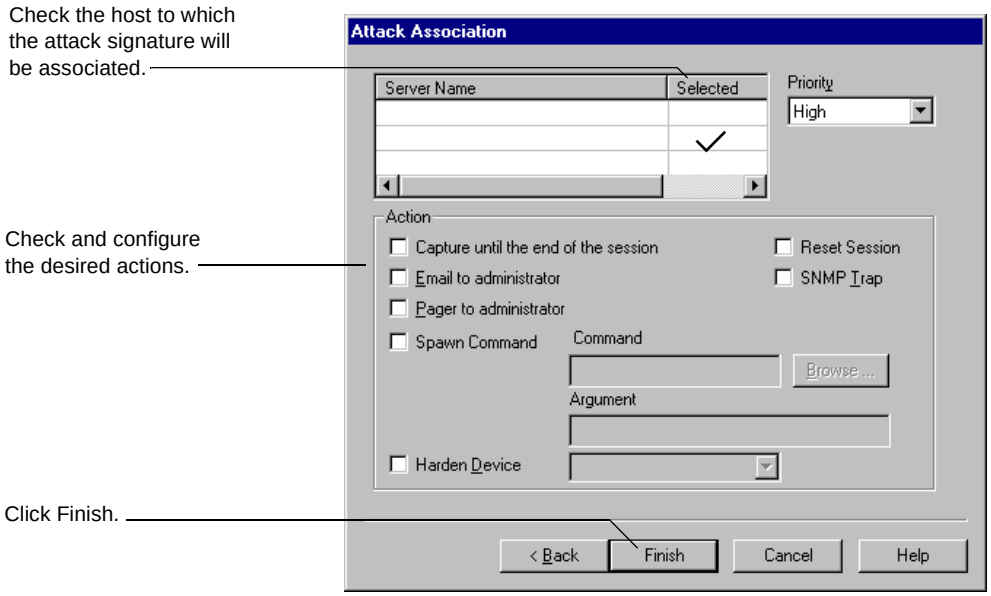


Figure 7-14: Attack Association Dialog Box

9. In the **Selected** column, select the host to which the attack signature will be associated.

   The attack signature will be associated with the checked host.

10. In the **Actions** box, check and configure, if necessary, the desired response actions.

11. When finished, click **Finish**.

    The attack signature is added to the list of available attack signatures and associated with the selected host.

Attack Signature Tutorials

With time and practice you can learn to create new attack signatures for NetProwler to use in identifying network-based attacks. AXENT has included three tutorials to give you experience and teach you the fundamental skills of creating attack signatures.

Prerequisite knowledge is required for creating new attack signatures. Before creating new attack signatures, you should have a solid understanding of the application and protocols used in the attack. For example, to accurately determine the nature of a particular client/server command in a custom application, you should know how the command is communicated over the network, including the hexadecimal and ASCII command itself, and also the offset (location) at which that command occurs in a session. The greater your knowledge of the application and protocols is, the more powerful the attack signature detection will be.

In addition, before starting the tutorials, you should be familiar with NetProwler's Attack Signature Definition tool, including:

- Search Primitives
- Value Primitives
- Reserved Keywords
- Expression Operators
- Expressions

For a description of each of these features, please read *Understanding the Attack Signature Definition Tool* on page 7.5.

Creating a Data-specific (FTP) Attack Signature

The FTP attack signature created in this example will search for an administrative password in an FTP session. Any user on the LAN trying to use this password to log into the FTP server will trigger this attack signature. The attack signature will be configured to reset (terminate) the attacker's session.

Optionally, you can configure an administrator's system to be an authorized host, meaning that when the administrator logs in to the FTP site as an administrator from the administrator's system, they will be exempt from NetProwler detection and reporting—no alarms or actions will be triggered. (To test the Authorized Host feature, you will need two FTP clients on two separate hosts.)

The following graphic illustrates the desired configuration for this attack signature.

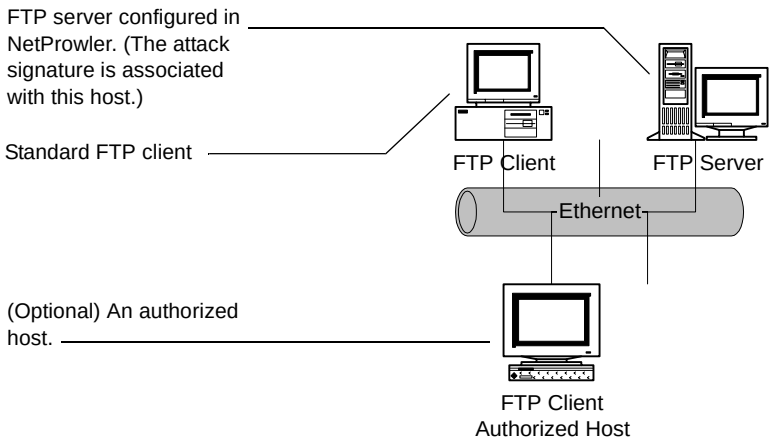


Figure 7-15: FTP Host Configuration

The tutorial will walk you through the steps of configuring the attack signature, associating it with the FTP server, and triggering the attack. Before continuing, please review the prerequisites for creating and executing this attack signature.

Prerequisites

To create and test this attack, you will need:

- Access over the network to an FTP server
- A user account on that server
- An FTP client such as the one included with Windows NT
- The FTP server entered into the NetProwler Address Book. The FTP server can be added automatically using the NetProwler Profiler or manually. For instructions on how to enter a system into NetProwler, see *Chapter 4: Building the Address Book.*
- (Optional) An administrator's system with an FTP client entered into the NetProwler Address Book (This system will be configured as an authorized user and be used to demonstrate how NetProwler excludes authorized users from detection and reporting.)

To create the FTP_Password attack signature:

1. Ensure that you have met the prerequisites described above.
2. In the NetProwler console, go to the **Configure** tree, and then expand the **Custom Attacks** and **Attack Definition** branches.

   The list of attack signatures should be visible.
3. Click **Add New**.

The Attack Signature Definition dialog box appears.

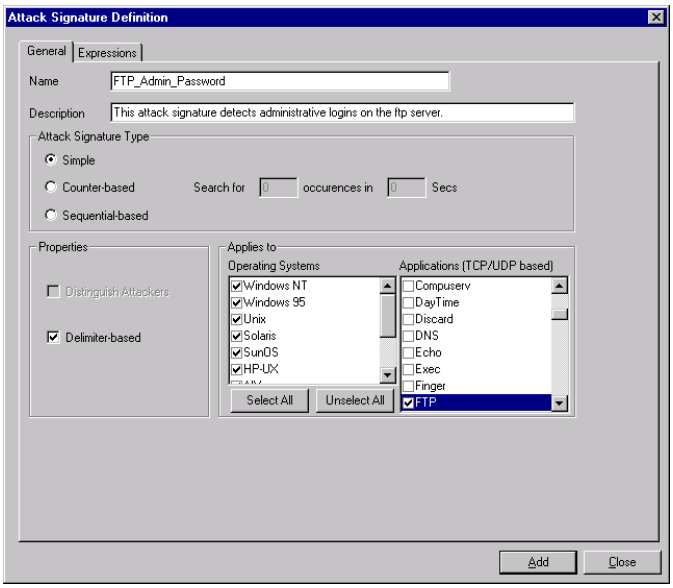


Figure 7-16: Attack Signature Definition Dialog Box

4. In the **Name** field, type "**FTP_Admin_Password**."
5. In the **Description** field, type the following description:

   This attack signature detects administrative logins on the ftp server.

6. In the **Attack Signature Type** box, select **Simple**.
7. In the **Properties** box, check **Delimiter-based**.
8. In the **Applies To: Operating Systems** box, click the **Select All** button since this attack is operating system independent.
9. In the **Applies To: Applications (TCP/UDP based)** box, scroll down and check **FTP**.
10. Click on the **Expressions** tab.

The Search Primitive tab should be visible.

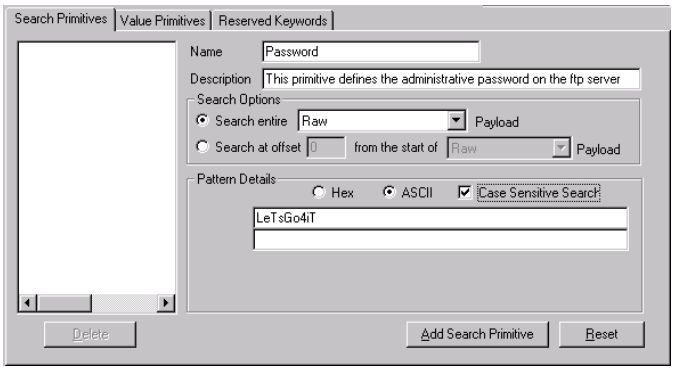


Figure 7-17: Search Primitive Tab

11. In the **Name** box, type "**Password**."
12. In the **Description** field, type the following description:

    This primitive defines the administrative password on the ftp server.

13. In the **Search Options** box, select **Search entire Raw Payload**.
14. In the **Pattern Details** box, select the **ASCII** radio button, and type the administrative password in the first available field.
15. (Optional) If the password uses varying case (upper and lower case characters), check the **Case Sensitive Search** check box.
16. Click **Add Search Primitive**.

    The configured search primitive is added to the list.

17. Drag and drop the configured search primitive from the list box to the Expressions box.

The following graphic illustrates the Expression box.

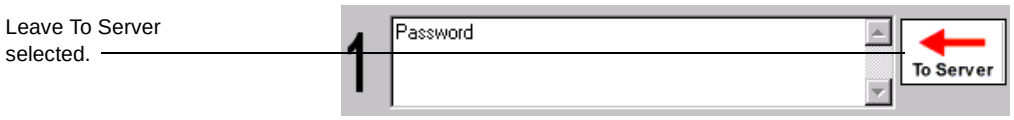


Figure 7-18: Expression box

18. Click **Add**, **Close**, and then **Apply**.

    The FTP_Password attack signature is added to the list of available attack signatures. You must now associate this attack signature with the FTP server.

19. Associate the FTP_Password attack signature with the FTP server and configure it to reset the session when detected.

    Optionally, configure an administrator's system as an authorized host. For instructions on how to associate an attack signature with a host and configure an administrator's system as an authorized host, see *Associating Attack Signatures Manually* on page 6.13.

    The FTP_Password attack signature is created and associated with the FTP server. The next step is to trigger the attack and monitor the results using NetProwler's Alarms feature.

To trigger the FTP_Password attack:

1. Start the FTP client software.
2. Attempt to logon to the FTP server.

   Be sure to type the same password configured in the FTP_Password attack signature.

   The attack is triggered.

To view the FTP_Password attack in NetProwler:

1. In the **Monitor** tree, select the **Alerts** branch.

   Does the FTP_Password attack appear in the list?

2. In the **Monitor** tree, expand the **Attacks** branch, and select **Custom Attacks**.

   Does the attack appear in this list?

   If the attack does not appear, troubleshoot the attack signature making sure it was configured properly and that the attack signature was properly associated with the FTP server. Ensure that NetProwler monitoring is started and that all changes were saved and activated by clicking the Apply buttons wherever changes were made.

Creating a Network-specific (LAND) Attack Signature

The LAND attack is a well-known attack where a single malformed packet is sent to a router, packet forwarding device, or host on the network. In this packet, the source IP address and destination IP address are the same. Routers attempt to forward the packet to themselves repeatedly in an endless loop. If many such packets are sent to the target device, it becomes so busy forwarding packets to itself that it is not able to forward legitimate traffic. Most machines crash when attacked. Any platform using the TCP/IP protocol is susceptible to this type of attack.

Prerequisites

The LAND attack is not easily reproducible and causes crashes on hosts and network devices. Therefore, steps to define the attack signature are shown, but instructions for triggering the attack are not included in this tutorial.

To create a network-specific (LAND) attack signature:

1. In the **Configure** tree, expand the **Custom Attacks** branch, and select **Attack Definition**.

   The list of attack signatures should be visible.

2. Click **Add New**.

   The Attack Signature Definition dialog box appears.

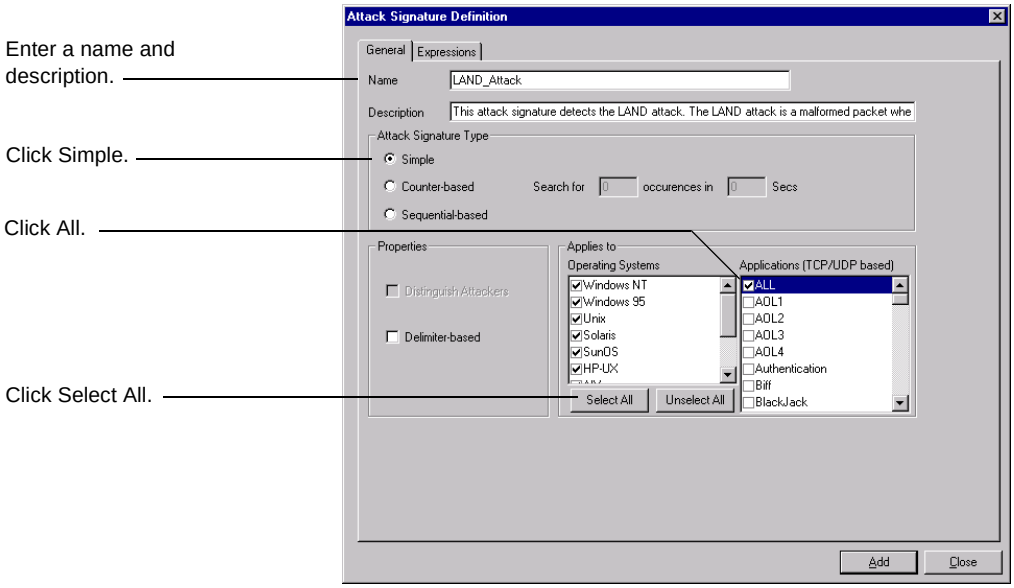


Figure 7-19: Attack Signature Definition Dialog Box

3. In the **Name** field, type **LAND_Attack**.
4. In the **Description** field, type the following description:

   This attack signature detects the LAND attack. The LAND attack is a malformed packet where the IP destination and source addresses are the same.

5. In the **Attack Signature Type** box, select **Simple**.
6. In the **Applies To: Operating Systems** box, click **Select All**.

7. In the **Applies To: Applications (TCP/UDP based)** box, check **All**.
8. Click the **Expressions** tab.

   The Expressions tab appears.

Build the expression here.

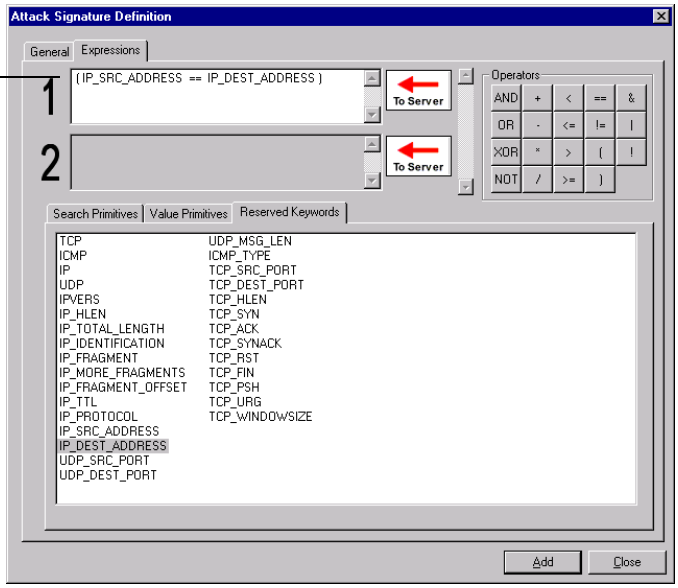


Figure 7-20: Expressions Tab

9. Select the **Reserved Keywords** tab.
10. In the **Operators** box, click the **Beginning Parenthesis** button.
11. Drag the **IP_SRC_ADDRESS** keyword to the Expression box and place it directly after the beginning parenthesis.
12. Place the cursor after IP_SRC_ADDRESS, and then click the **Equal To** operator.
13. Drag the **IP_DEST_ADDRESS** keyword to the Expression box and place it after the Equal To operator.
14. Place the cursor after IP_DEST_ADDRESS, and then click the **Ending Parenthesis** button.

The expression should appear as follows.

(IP_SRC_ADDRESS == IP_DEST_ADDRESS)

NOTE

Some implementations of the LAND attack specify the same port as well as the same IP address. To modify the above expression to detect this implementation, modify the expression as follows:

((IP_SRC_ADDRESS == IP_DEST_ADDRESS) AND (IP_SRC_PORT == IP_DEST_PORT))

15. Click **Add**, **Close**, and then **Apply**.

    The LAND_Attack attack signature is added to the list of available attack signatures.

16. Associate the LAND_Attack attack signature with the desired hosts.

    For instructions on how to associate an attack signature with a host, see *Associating Attack Signatures Manually* on page 6.13.

    The LAND_Attack attack signature is created and associated with the desired hosts.

Creating a Counter-based (Failed Logins) Attack Signature

Counter-based attack signatures are triggered by repeated occurrences of the same event. NetProwler can monitor any TCP/IP protocol, look for a specific occurrence, and remember the state information about the session. The state information provides a context that allows NetProwler to detect an action that happens a certain number of times within a specified period of time.

Multiple failed logins on the same system are tell tale signs of an attacker's attempts to gain access to a remote system. In this exercise, you will learn how to create an attack signature that detects three failed logins using Telnet.

Prerequisites

To create and test this attack, you will need:

- Access over the network to an telnet server (It is not necessary to have an account on that server.)
- An telnet client such as the one included with Windows NT
- The telnet server entered into the NetProwler Address Book. (The telnet server can be added automatically using the NetProwler Profiler or manually. For instructions on how to enter a system into NetProwler, see *Chapter 4: Building the Address Book*.)

To create the Telnet_3Failed_Logins attack signature:

1. In the **Configure** tree, expand the **Custom Attacks** branch, and select **Attack Definition**.

   The list of attack signatures should be visible.

2. Click **Add New**.

The Attack Signature Definition dialog box appears.

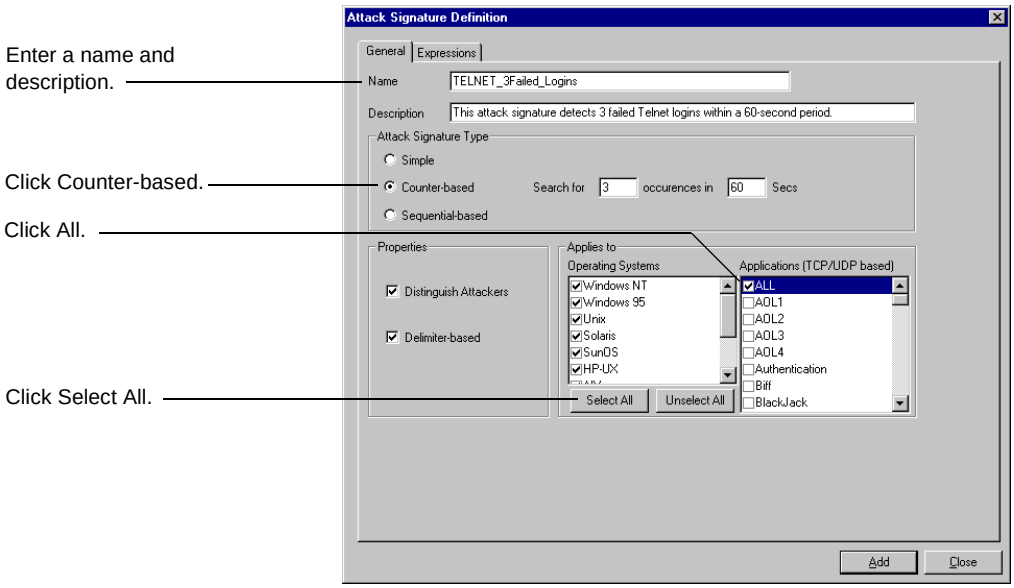


Figure 7-21: Attack Signature Definition Dialog Box

3. In the **Name** field, type "**Telnet_3Failed_Logins**."
4. In the **Description** field, type the following description:

   This attack signature detects 3 failed Telnet logins within a 60 second period.

5. In the **Attack Signature Type** box, select **Counter-based**, and configure it to search for "**3**" occurrences in "**60**" seconds.
6. In the **Properties** box, check the **Distinguish Attackers** check box.

   The Distinguish Attackers tells NetProwler that a set of occurrences is an attack only if the actions all come from the same IP address within the specified period of time. In this case, we have configured NetProwler so that three failed login attempts from the same user within 60 seconds triggers this attack signature.

7. Also in the **Properties** box, check the **Delimiter-based** check box.

   (Telnet is a delimiter-based application. Telnet, rLogin, and rSH use a dumb terminal that echoes characters one at a time to the terminal server. Selecting Delimiter-based tells NetProwler that it must wait for the carriage return / line feed before processing the information that was transmitted. This option is required for these protocols.)

8. In the **Applies To: Operating Systems** box, click **Select All**.

9. In the **Applies To: Applications (TCP/UDP based)** box, check **Telnet**.

10. Click the **Expressions** tab.

    The Expressions tab appears.

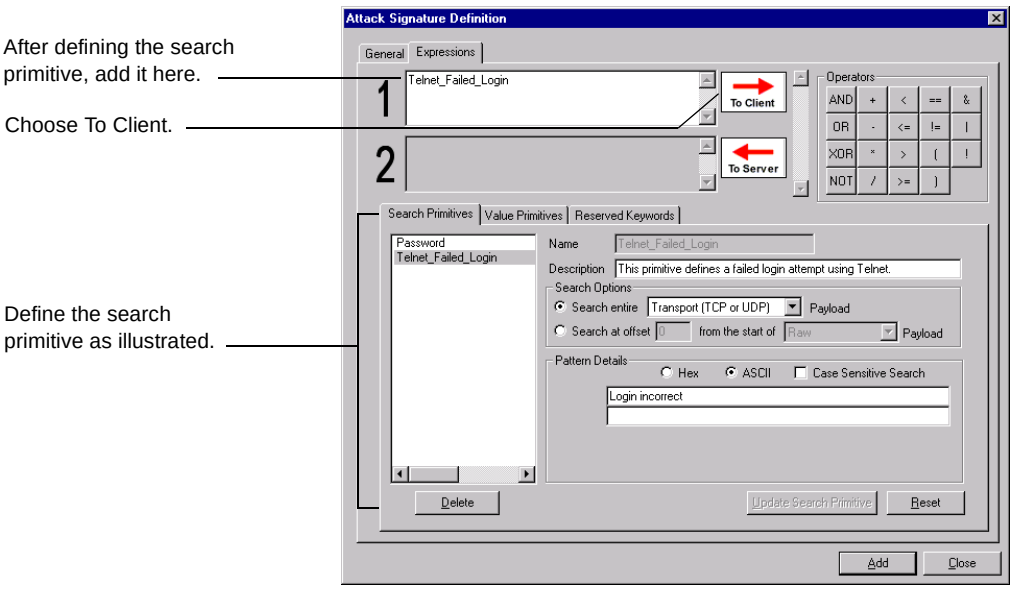


Figure 7-22: Expressions Tab

11. On the **Search Primitive** tab, create a new search primitive named "Telnet_3Failed_Logins."

12. In the **Description** field, type the following description:

    This primitive defines a failed login attempt using Telnet.

13. In the **Search Options** box, select **Search entire Transport (TCP or UDP) Payload**.
14. In the **Pattern Details** box, select the **ASCII** radio button.
15. In the first provided field, type the response the telnet server uses to tell the user that the login attempt was unsuccessful.

    If you do not know this response, start your telnet client and deliberately fail a login attempt to the target server.

    Examples include:

    Login incorrect

    Invalid login

    You entered an invalid login name or password.

16. Click **Add Search Primitive**.

    The Telnet_Failed_Logins search primitive is added to the list.

17. Drag the **Telnet_Failed_Logins** search primitive to the **Expression** box.

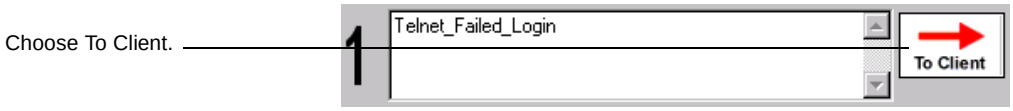


Figure 7-23: Expression Box

18. Click the **To Server** button once or until it reads **To Client**, as illustrated in the graphic above.

    This tells NetProwler the direction of the traffic; the server is sending the failed login message to the client.

19. Click **Add**, **Close**, and then **Apply**.

The TELNET_3Failed_Logins attack signature is added to the list of available attack signatures.

20. Associate the Telnet_3Failed_Logins attack signature with the telnet server.

    For instructions on how to associate an attack signature with a host, see *Associating Attack Signatures Manually* on page 6.13.

    The Telnet_3Failed_Logins attack signature is created and associated with the desired hosts. The following instructions describe how to trigger the attack signature.

To trigger the Telnet_3Failed_Logins attack:

1. Start the telnet client software.
2. Specify the target telnet server.
3. When prompted for the **Login** and **Password**, enter bogus values, and then press **Enter**.

   The failed login message appears.
4. Repeat **Step 3** two more times within a 60 second period or time.

   The Telnet_3Failed_Logins attack incident should appear in the NetProwler Monitor pane.

To view the Telnet_3Failed_Logins attack in NetProwler:

1. In the **Monitor** tree, select the **Alerts** branch.

   Does the Telnet_3Failed_Logins attack appear in the list?

2. In the **Monitor** tree, expand the **Attacks** branch, and select **Custom Attacks**.

   Does the attack appear in this list?

   If the attack does not appear, troubleshoot the attack signature making sure it was configured properly and that the attack signature was properly associated with the Telnet server. Ensure that NetProwler monitoring is started and that all changes were saved and activated by clicking the Apply buttons wherever changes were made.

Securing Network Resources

Overview

Securing network resources against malicious tampering or theft remains a major reason for using an intrusion detection tool. NetProwler helps you to secure to integrity and reliability of your network resources by monitoring web server, ftp server, DNS, and router configuration files for malicious tampering. NetProwler also lets you impose access time limitations on the TCP/IP based applications on your configured systems. Chapter 8 provides instructions on how to configure NetProwler to monitor these resources. Chapter topics include:

- Securing Web server resources
- Securing FTP server resources
- Securing DNS hostnames
- Securing router configuration files
- Limiting access to network resources

Securing Web Server Resources

NetProwler helps secure the integrity and reliability of your web server by monitoring all file-based resources. At user-determined intervals, NetProwler can compare the HTML pages, scripts, images, and other static information on a web server and compare it against a mirror server. NetProwler performs a byte-by-byte comparison of every designated file on the web server with the files on a mirror server.

To check file consistency on a web server, NetProwler requires an up-to-date mirror server to compare with the web server. Both the web server and the mirror server must be added to the address book.

To secure Web server resources:

1. In the **Configure** tree, expand the **Consistency** branch, and click **Web**.

   The **Configure** pane displays the web server systems that NetProwler will monitor.

2. Click **Add New**.

The Web Consistency Check dialog box appears.

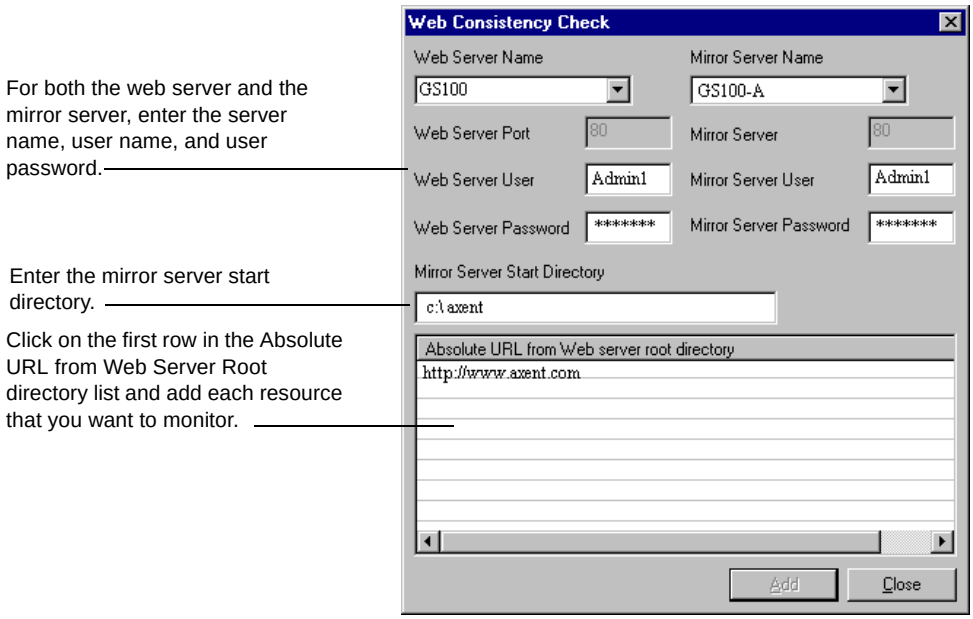


Figure 8-1: Web Consistency Check dialog box

3. In the **Web Server Name** list box, select the name of the web server to check.
4. In the **Mirror Server Name** list box, select the name of the mirror server.

   If the web or mirror server doesn't appear in the list, check to ensure that you have added it to the address book.

   NetProwler assumes that the Port number on the web and mirror servers is 80. This option is preset for you.
5. In the **Web Server User** and **Mirror Server User** boxes, type the user name for the web server and mirror server .
6. In the **Web Server Password** and **Mirror Server Password** boxes, type the password for the web server and mirror server.

7. In the **Mirror Server Start Directory** box, type the path name of the Start directory.
8. In the **Absolute URL from Web Server Root Directory**, add each resource that you wish to monitor by clicking on the open cell.
9. When you are finished adding resources, click **Add** to activate your choices.
10. In the **Configure** pane, schedule the frequency that NetProwler will check the resources by clicking **Monthly**, **Weekly**, or **Daily**, and then selecting the time of day, and the day of month or day of week as appropriate.
11. Click **Apply** to complete the scheduling.

Modifying a Web Server Consistency Check Entry

NetProwler lets you modify a web server consistency check entry to accommodate changing network circumstances.

To modify a Web server consistency check entry:

1. In the **Configure** tree, expand the **Consistency** branch, and click **Web**.

   The **Configure** pane displays the web server systems that NetProwler will monitor.

2. Click the entry that you want to modify.

   The Edit Web Server Consistency Check dialog box appears.

Click an entry in the Absolute URL from Web server root directory to edit or delete it. Click the first empty row to add a new URL to the consistency check.

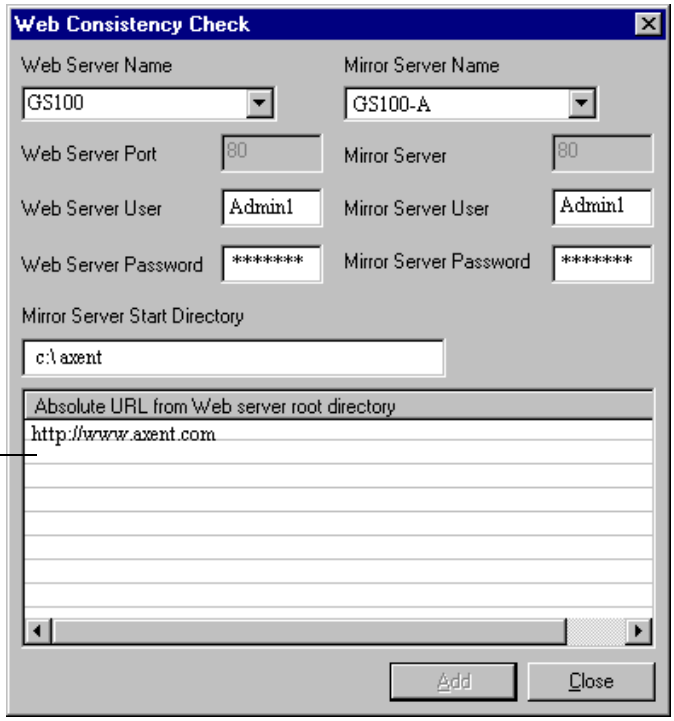


Figure 8-2: Edit Web Server Consistency Check Dialog Box

3. To edit an entry, click it and type the new information.
4. To delete an entry, click it and press the **Delete** key.
5. To add a new entry, click the first blank row and type in the URL information.
6. Click **Update** and then **Apply**.

Deleting a Web Server Consistency Check Entry

You can delete a web server consistency check entry from the Configure pane when network circumstances change.

To delete a Web server consistency check entry:

1. In the **Configure** tree, expand the **Consistency** branch, and click **Web**.

   The Configure pane displays the web server systems that NetProwler will monitor.
2. Click the entry.
3. Click **Delete** and then **Apply**.

   NetProwler deletes the entry from the Configure pane.

Securing FTP Server Resources

An organization's ftp server is often the first site of contact for outside hosts. Attackers may try to penetrate or compromise the ftp server to gain further access into the network. They may maliciously replace files on the ftp server with different files having the same names, upload a file containing a virus, or otherwise tamper with files on the server.

NetProwler lets you ensure that the files stored on an ftp server have not been tampered with. It performs a byte-by-byte comparison of every designated file on the ftp server with the files on an ftp mirror server.

To check file consistency on a ftp server, NetProwler requires an up-to-date mirror server to compare with the ftp server. Both the ftp server and the mirror server must be added to the address book.

To secure FTP server resources:

1. In the **Configure** tree, expand the **Consistency** branch, and click **FTP**.

   The Configure pane displays the ftp server systems that NetProwler will monitor.

2. Click **Add New**.

The FTP Consistency Check dialog box appears.

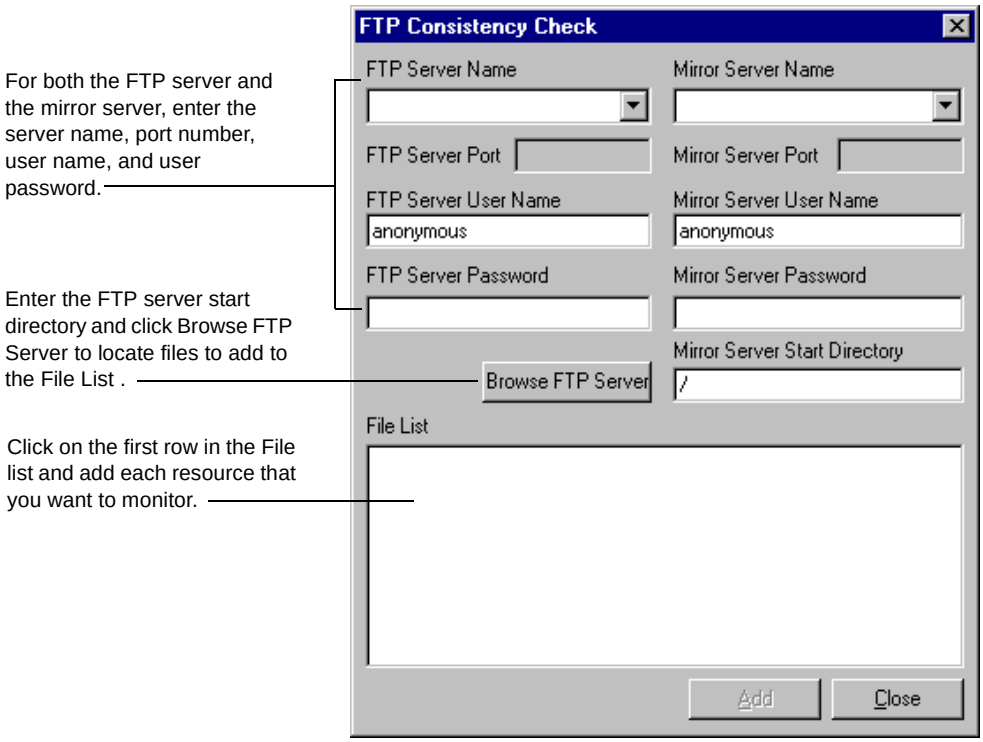

For both the FTP server and the mirror server, enter the server name, port number, user name, and user password.
Enter the FTP server start directory and click Browse FTP Server to locate files to add to the File List .
Click on the first row in the File list and add each resource that you want to monitor.
FTP Consistency Check
FTP Server Name
Mirror Server Name
FTP Server Port
Mirror Server Port
FTP Server User Name
anonymous
Mirror Server User Name
anonymous
FTP Server Password
Mirror Server Password
Mirror Server Start Directory
/
Browse FTP Server
File List
Add
Close

Figure 8-3: FTP Consistency Check Dialog Box

3. In the **FTP Server Name** box, select the name of the web server to check.
4. In the **Mirror Server Name** box, select the name of the mirror server.

   If the ftp or mirror server does not appear in the list, check to ensure that you have added it to the address book.
5. In the **FTP Server Port** and **Mirror Server Port** boxes, type the port numbers for the ftp server and mirror server.
6. In the **FTP Server User** and **Mirror Server User** boxes, type the user name for the ftp server and mirror server.

7. In the **FTP Server Password** and **Mirror Server Password** boxes, type the password for the ftp server and mirror server.
8. In the **Mirror Server Start Directory** box, type the path name of the Start directory on the mirror server.
9. Use the **Browse FTP Server** button to search the ftp server for directories to add to the File List.
10. In the **File List**, add each resource that you wish to monitor by clicking on an open cell.

Directory and files names added to the File List should not contain spaces.

11. When you are finished adding resources to the **File List**, click **Add** to activate your choices.
12. In the **Configure** pane, schedule the frequency that NetProwler will check the resources by clicking **Monthly**, **Weekly**, or **Daily**, and then selecting the time of day, and the day of month or day of week as appropriate.
13. Click **Apply** to complete the scheduling.

Modifying an FTP Server Consistency Check Entry

NetProwler lets you modify an ftp server consistency check entry to accommodate changing network circumstances.

To modify an FTP server consistency check entry:

1. In the **Configure** tree, expand the **Consistency** branch, and click **FTP**.

   The Configure pane displays the ftp server systems that NetProwler will monitor.
2. Click the entry that you want to modify.

The Edit FTP Server Consistency Check dialog box appears.

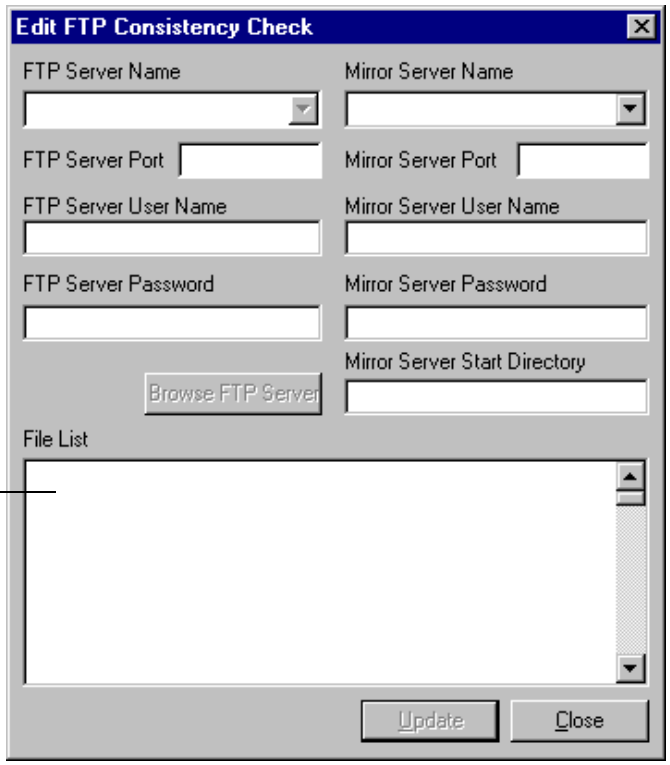

Edit FTP Consistency Check
FTP Server Name
Mirror Server Name
FTP Server Port
Mirror Server Port
FTP Server User Name
Mirror Server User Name
FTP Server Password
Mirror Server Password
Mirror Server Start Directory
Browse FTP Server
File List
Update
Close
Click an entry in the File List to edit or delete it.
Click the first empty row to add a File to the consistency check.

Figure 8-4: Edit FTP Server Consistency Check Dialog Box

3. To edit an entry, click it and type the new information. (The FTP Server name, FTP Server Port, and Mirror Server Port entries cannot be edited.)
4. To delete an entry, click it and press the **Delete** key.
5. To add a new entry, click the first blank row and type in the new information.
6. Click **Update** and then **Apply**.
7. NetProwler updates the Configure pane.

Deleting an FTP Server Consistency Check Entry

You can delete a ftp server consistency check entry from the Configure pane when network circumstances change.

To delete a FTP server consistency check entry:

1. In the **Configure** tree, expand the **Consistency** branch, and click **FTP**.

   The Configure pane displays the ftp server systems that NetProwler will monitor.

2. Click the entry.

3. Click **Delete** and then **Apply**.

   NetProwler deletes the entry from the Configure pane.

Securing DNS Hostnames

A DNS hostname server presents another common target for intrusion attacks. DNS hostnames that have been tampered with can cause denial-of-service attacks or other undesirable consequences. For example, an attacker could change a world wide web hostname to map to the web server of a competitor.

At periodic intervals, NetProwler tests the DNS entries that are live on the network to ensure that DNS hostnames have not been remapped to incorrect IP addresses. NetProwler tests DNS entries by comparing its list of host names and the IP addresses to which they correspond with the DNS entries currently on the network.

To secure the DNS table:

1. In the **Configure** tree, expand the **Consistency** branch, and click **DNS**.

   The Configure pane displays the DNS servers that NetProwler will monitor.

2. Click **Add New**.

   The DNS Consistency Check dialog box appears.

Click name of the DNS server in the DNS Server Name box.

Add the DNS host names and IP addresses that have been assigned to these host names.

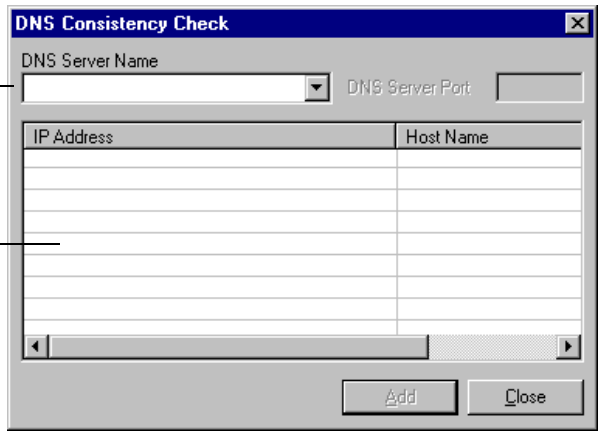


Figure 8-5: DNS Consistency Check Dialog Box

3. In the **DNS Server Name** box, click the server on which you want to perform consistency checking.
4. Click the first open row in the **IP Address** column, and then type the DNS host name to be monitored. NetProwler adds the IP address associated with the host name. Repeat for all host names that you want to consistency check.
5. When you are finished adding resources, click **Add** to activate your choices.
6. In the **Configure** pane, schedule the frequency that NetProwler will check the resources by clicking **Monthly**, **Weekly**, or **Daily**, and then selecting the time of day, and the day of month or day of week as appropriate.
7. Click **Apply** to complete the scheduling.

Modifying a DNS Host Name Entry

NetProwler lets you modify a DNS host name entry by adding or deleting IP addresses from the list of addresses to check.

To modify a DNS host name entry:

1. In the **Configure** tree, expand the **Consistency** branch, and click **DNS**.

   The Configure pane displays the DNS servers that NetProwler will monitor.

2. Click the entry that you want to modify.

   Or

   Right-click the entry and then click **Modify**.

   The Edit DNS Consistency Checking dialog box appears.

Add a new IP address by clicking the first empty row and typing the new IP address.
or
Delete an existing IP address by clicking it and then pressing the Delete key.

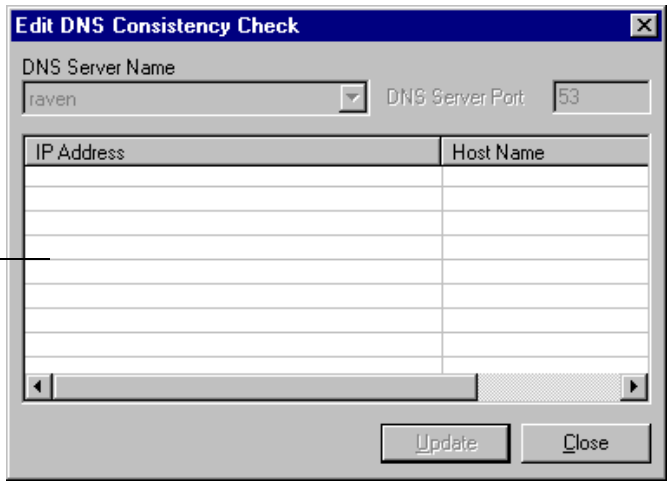


Figure 8-6: Edit DNS Consistency Checking Dialog Box

3. Add a new IP address by clicking the first empty row and typing the new IP address.
4. Delete an existing IP address by clicking it and then pressing the **Delete** key.

5. Click **Update**.

   The Edit DNS Consistency Checking dialog box closes and NetProwler returns to the Configure pane.

6. Click **Apply** to activate the changes.

Deleting a DNS Consistency Check Entry

You can delete a DNS Consistency Check entry when you no longer need to perform consistency checking on a DNS name server.

To delete a DNS consistency check entry:

1. In the **Configure** tree, expand the **Consistency** branch, and click **DNS**.

   The Configure pane displays the DNS servers that NetProwler will monitor.

2. Click the DNS entry that you want to delete.

3. Click **Delete** and then **Apply**.

   NetProwler deletes the entry from the Configure pane.

Securing Router Configuration Files

Routers connect local area networks to each other. They also filter messages and packets and forward them to different systems and devices on the network. Therefore, a necessary part of network security is ensuring that the routers are protected from intrusion attacks. For example, an attacker having gained access to routing controls on the network could perform a denial of service attack by routing all network traffic to an invalid gateway, resulting in the interruption of normal network service.

NetProwler helps you to protect your routers from intrusion attacks by verifying that the routing set up on the network has not been modified without authorization.

To secure router configuration files:

1. In the **Configure** tree, expand the **Consistency** branch, and click Router.

   The Configure pane displays the routers that NetProwler will monitor.

2. Click **Add New**.

The Router Consistency Check dialog box appears.

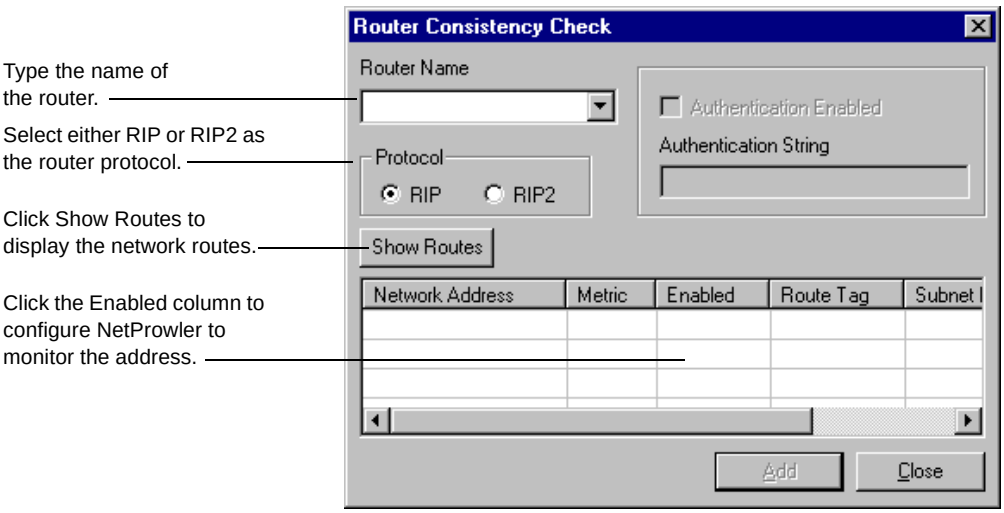


Figure 8-7: Router Consistency Check Dialog Box

3. In the **Router Name** box, click the router on which you want to perform consistency checking.
4. In the **Protocol** group, click **RIP** or **RIP2** to indicate the router's protocol.
5. (Optional) If RIP2 protocol is chosen, you have the option to enable authentication by clicking the **Authentication Enabled** check box and typing in an authentication string in the **Authentication String** box.
6. Click **Show Routes** to display the network routes in the **Network Address** column.
7. For each network address, click the **Enabled** column to instruct NetProwler to monitor that address.
8. When you are finished adding resources, click **Add** to activate your choices.

Modifying a Router Consistency Check Entry

NetProwler lets you modify a router entry by enabling or disabling network addresses to check.

To modify a router's network address entry:

1. In the **Configure** tree, expand the **Consistency** branch, and click **Router**.

   The Configure pane displays the routers that NetProwler will monitor.

2. Click the entry that you want to modify.

   Or

   Right-click the entry, and then click **Modify**.

   The Edit Router Consistency Checking dialog box appears.

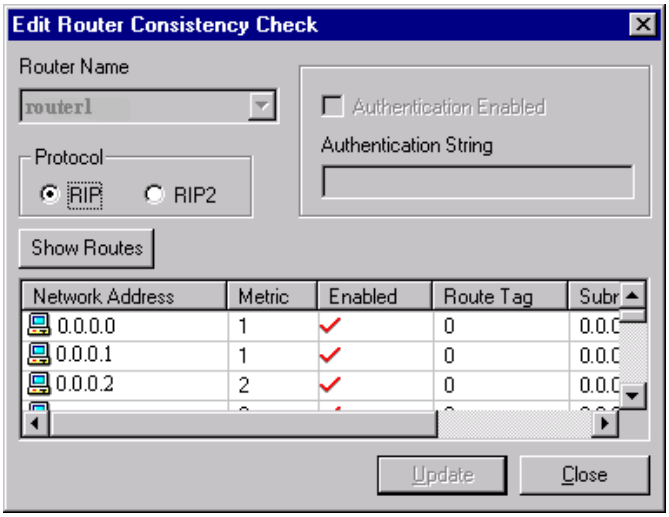


Figure 8-8: Edit DNS Consistency Checking Dialog Box

3. Enable or disable a network address by clicking the **Enabled** column.

4. Click **Update**.

   The Edit DNS Consistency Checking dialog box closes and NetProwler returns to the Configure pane.

5. Click **Apply** to save and activate the changes.

Deleting a Router Consistency Check Entry

You can delete a Router Consistency Check entry when you no longer need to perform consistency checking on a router.

To delete a router consistency check entry:

1. In the **Configure** tree, expand the **Consistency** branch, and click **Router**.

   The Configure pane displays the routers that NetProwler will monitor.

2. Click the router entry that you want to delete.

3. Click **Delete** and then **Apply**.

   NetProwler deletes the entry from the Configure pane.

Limiting Access to Network Resources

NetProwler lets you stop traffic to one or more TCP/IP based applications on a monitored system. You can limit traffic to one or more systems on the network during certain times of the day or certain days of the week. NetProwler can perform this function without modifying client or server workstations.

You can use NetProwler's limit access feature when network services are provided for internal use only. For example, access to an intranet FTP server that contains sensitive information can be restricted to weekdays. Once you create a time access entry, you can modify or delete the entry when necessary.

To limit access to network resources:

1. In the **Configure** tree, click **Access**.

   The Configure pane displays the systems that NetProwler limits access to, the TCP/IP based applications that are restricted, and the days and times that NetProwler allows access.

2. Click **Add New**.

The New Time of Day Access Entry dialog box appears.

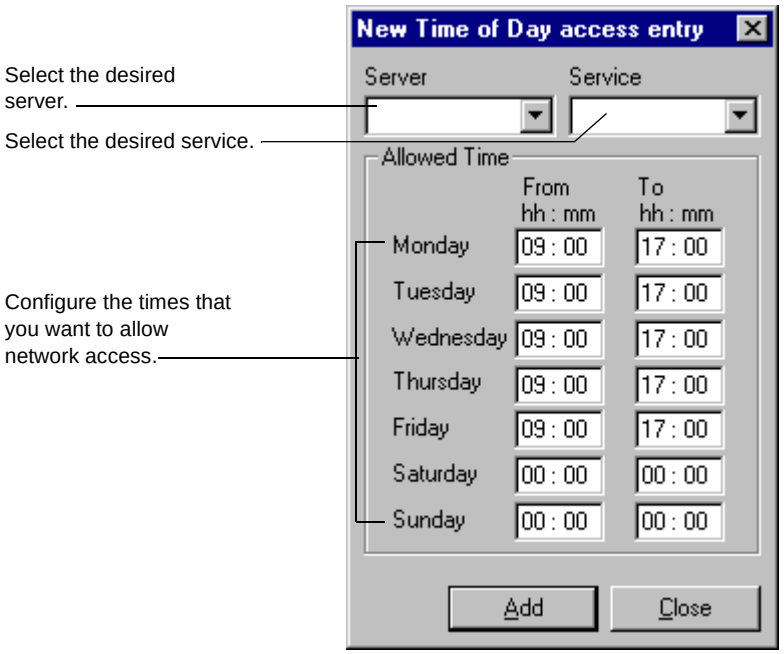

Select the desired server.
Select the desired service.
Configure the times that you want to allow network access.
New Time of Day access entry
Server
Service
Allowed Time
From hh : mm
To hh : mm
Monday 09 : 00 17 : 00
Tuesday 09 : 00 17 : 00
Wednesday 09 : 00 17 : 00
Thursday 09 : 00 17 : 00
Friday 09 : 00 17 : 00
Saturday 00 : 00 00 : 00
Sunday 00 : 00 00 : 00
Add
Close

Figure 8-9: New Time of Day Access Entry

3. In the **Server** box, click on the system on which you want to limit access days and times.
4. In the **Service** box, click the TCP/IP based services that you want to restrict. Click **All** to restrict TCP/IP based services.
5. For each day of the week in the **Allowed Time** group, specify the hours during which this application is allowed. For example, to restrict use during the hours of 11:00 a.m. to 1:00 a.m., enter 14:00 in the **From** box and 10:00 in the **To** box. (The Limit Access feature uses military time.)

   To restrict an entire day, specify 00:00 in both the **From** and the **To** box.

To restrict multiple, but not all, applications during specific times, create multiple Time of Day restrictions for the same server.

6. When you are finished adding resources, click **Add** to add the server to the **Configure** pane. Click **Close** to close the dialog.

   The Configure pane displays your settings

7. In the **Configure** pane, click **Apply** to activate the settings.

Modifying a Limit Access Entry

NetProwler lets you modify a time access entry to accommodate changing network circumstances.

To modify a limit access entry:

1. In the **Configure** tree, click **Access**.
2. The Configure pane displays the systems that NetProwler limits access to, the TCP/IP based applications that are restricted, and the days and times that NetProwler allows access.
3. Click on the entry.

   Or

   Right-click on the entry and click **Modify**.

The Edit Host Entry dialog box appears.

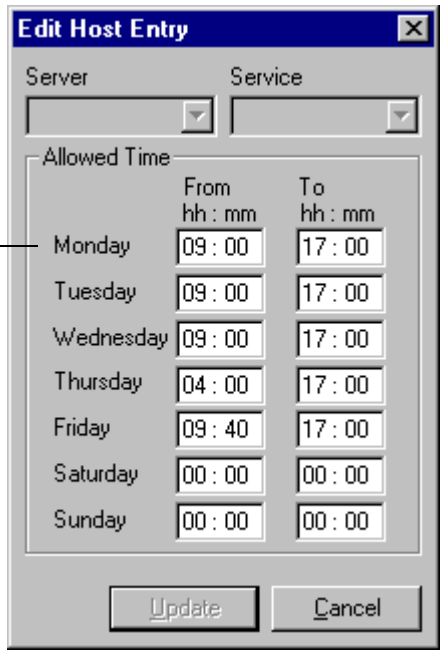

Edit Host Entry
Server
Service
Allowed Time
From hh : mm
To hh : mm
Monday 09 : 00 17 : 00
Tuesday 09 : 00 17 : 00
Wednesday 09 : 00 17 : 00
Thursday 04 : 00 17 : 00
Friday 09 : 40 17 : 00
Saturday 00 : 00 00 : 00
Sunday 00 : 00 00 : 00
Update
Cancel
Make the desired changes.

Figure 8-10: Edit Host Entry Dialog box

4. For each day and time that you want to modify, specify the new allowed times in the **From** and **To** boxes.
5. Click **Update**.

   The Configure pane displays the modified entry.
6. Click **Apply** to activate the changes.

Deleting a Limit Access Entry

When the circumstances that required access limits change or no longer apply, you can delete an entry from the Configure pane.

To delete a limit access entry:

1. In the **Configure** tree, click **Access**.
2. The Configure pane displays the systems that NetProwler limits access to, the TCP/IP based applications that are restricted, and the days and times that NetProwler allows access.
3. Click on the entry that you want to delete.
4. Click **Delete** and then **Apply**.

   NetProwler deletes the entry from the Configure pane.

Monitoring Attacks and Network Conversations

Overview

Network conversations, also sometimes referred to as network *sessions*, are communications channels opened up between two computers, such as a telnet session or a system accessing a POP3 server to retrieve e-mail. If the security administrator believes that an unauthorized conversation is occurring, NetProwler can monitor specified types of network conversations, log when they start and stop, capture the contents of such sessions, and even terminate them,

Additionally, common types of connections to systems monitored by NetProwler can be captured and replayed in a mode that shows just what the user who makes the connection sees (rather than low-level packet capture, which is the method used to capture all other types of conversations).

NetProwler has a predefined list of conversation types, but new types can be created to accommodate the type of traffic you have on your network.

In this chapter, you will learn how to:

- Monitor attacks detected by NetProwler
- Configure NetProwler to monitor network conversations.
- Examine network conversations as they occur on your network.
- Terminate an unauthorized network conversation.
- Capture and replay a network conversation.

Monitoring Attacks that NetProwler Detects

Once you have configured NetProwler to detect certain kinds of attacks on particular machines, NetProwler begins logging each attack it detects. All attacks are shown as alerts and logged in the Alerts database. Additionally, alerts for Common attacks are monitored separately, and all the alerts for custom attacks are shown together in another place.

If you have specified that NetProwler should capture particular types of sessions (in the Edit Attack Association Details dialog box; see *Configuring NetProwler Actions* earlier in this chapter for more information), you can also view these captured sessions. Common attack types can be viewed in a format that looks like a user session.

Viewing All Alerts

When NetProwler detects an attack, the attack appears as an alert in the NetProwler Monitor window, which means that it also gets logged in the Alerts database. The Alerts icon (in the upper right of the NetProwler window) also flashes when new alerts have been added but not viewed.

The color of the Alerts icon depends on the priority of the detected attack. A flashing red icon indicates a high priority attack, while the blue or yellow icons indicate a medium or low attack.

If NetProwler detects more than one attack, the Alerts icon flashes the color of the highest priority. For example, if a high priority attack and a medium priority attack is detected, the Alerts icon will flash red. If a medium priority attack and a low priority attack is detected, the Alerts icon will flash blue.

The Alerts database is a Microsoft Access database that stores all the information NetProwler gathers about a network, including Attack alerts, Conversation starts and stops, Consistency problems, and so forth.

To view all alerts:

1. In the **Monitor** tree, click **Alerts**.
2. (Optional) If you want to see only alerts of a certain priority, click the **High**, **Medium**, and **Low** check boxes at the bottom of the **Monitor** window to turn those items on or off.

   The Monitor pane displays the latest alerts logged by NetProwler since it was started. It includes information on which system was attacked, which application port was attacked, the attack type, the attack date and time, the attack priority, and any additional information about the attack (this information varies, depending on the type of alert).

Resetting Alerts

You can reset the Monitor Alerts window to make it easier to see the most recent attacks. Resetting the Monitor Alerts window also clears the attacks that appear in the Attacks branch.

Resetting the Alerts window does not change what gets logged in the Alerts database. You can still view any alerts cleared from the Monitor Alerts window by generating a report or by querying the Alerts database.

To reset the Alerts window:

1. Click **Reset Alerts** in the Toolbar.
2. Click **Yes** to confirm that you want to reset the alert monitoring.

   The **Monitor Alerts** window is cleared.

Viewing Alerts by Attack Type

NetProwler logs an alert when it detects a configured attack. These alerts can be viewed together in the Alerts branch or by attack type in the Attacks branch. Alerts for the Common attacks can be viewed by the type of Common attack. For example, all Port Scan attacks can be viewed in one place, all SYN Flood attacks in another, and so forth. In addition, all the custom attacks can be viewed together under the Attacks, Custom Attacks branch.

To view alerts by attack type:

1. In the **Monitor** tree, expand the **Attacks** branch (if necessary), and then click any of the desired type of attack.

   For example, to view all Port Scan attacks, click Port Scan. To view all custom attacks, click the Custom Attacks branch.

   Any attacks of that type are shown in the **Monitor** pane, along with details relevant to that type of attack. The **Monitor** pane will not show any attacks if none has been detected.

Click on an attack in the Attacks branch and the Monitor Pane displays any detected occurrences of the attack.

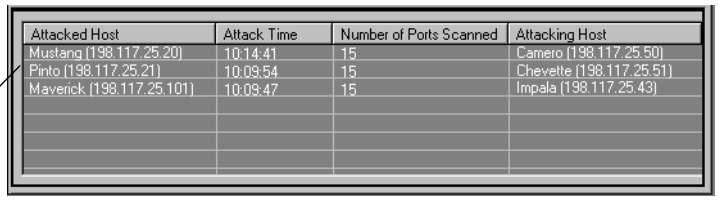


Figure 9-1: Monitor Pane - Port Scan Attack

Viewing Captured Attack Sessions

When you configure attack association details, you can specify that you want NetProwler to capture certain types of network attack sessions (see *Configuring NetProwler Actions* earlier in this chapter for more information). This is a good way to examine particular types of attacks so you can learn more about them, get more information about the nature of the attack, fine-tune attack signatures, create new attack signatures, and possibly use the data for legal prosecution purposes. Later you can view any of these captured sessions.

To view a captured attack session:

1. In the **Monitor** tree, expand **Attacks** (if necessary) and click **Captured Attack Sessions**.

   Any captured attack sessions appear in the **Monitor** window.

2. Double-click a session to view it.

   The captured session appears in a session window. Common session types (FTP, telnet, chat, SMTP, POP3, RSH, and rlogin) appear just as a user would see the session. All other types of sessions appear packet by packet in ASCII and hexadecimal format.

Configuring Conversation Monitoring

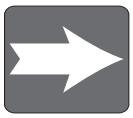
You can have NetProwler monitor particular conversation types (such as FTP, echo, POP3, etc.) or all conversation on any of the systems in the Address Book (for more information about setting up the Address Book, see *Chapter 4: Building the Address Book*).

Conversation monitoring is CPU intensive. You can improve NetProwler's performance by turning conversation monitoring on only when needed. This allows NetProwler to use the dedicated system's CPU resources for intrusion detection.

1. In the **Configure** tree, click **Conversations**.

   A list of NetProwler-monitored servers appears in the **Server Name** column of the **Configure** pane.

2. To enable conversation monitoring of particular applications (e.g., services), add check marks in the row of a system you want to monitor and in the column of the service you want to monitor.



The list of services is quite large. Use the horizontal scroll bar below this table to see the full list.

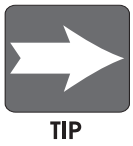
   Or

   To enable monitoring of all network conversations for a particular system, place a check mark in the **All** column next to that server name.

   Note that selecting **All** means that all network conversations this system has (whether connecting to or being connected to) will be monitored, not just those in the applications list.

3. Specify a length of time for purging sessions that are inactive or leave the default time of 60 minutes.

If you want every conversation start and stop to be logged in the Alerts database, place a check in the **Enable session start/stop logging** check box.



Depending on the system, this could result in a very large number of entries in the Alerts database. A large number of entries in the Alerts database could affect NetProwler's performance in generating reports or queries.

4. Click **Apply** (in the lower right of the **Configure** pane) to save and apply any changes you made.

Viewing Live Conversations

Since NetProwler provides a dynamic look at the state of your network, you can observe the network conversations that are occurring on the network in real time. NetProwler places seven of the most common types of network conversations (FTP, Telnet, IRC, SMTP, POP3, rSH, and rLogin) in their own categories, and places anything else it sees in the Generic category.

The common types of conversations are displayed in a way that shows what a user would see. All other conversation types are shown packet by packet, both in ASCII and in hex.

To view live network conversations:

1. In the **Monitor** tree, expand **Conversations** (if necessary) and select a conversation type (**Generic** to see anything not in one of the predefined categories).

   The list of current conversations of that type appears in the **Monitor** pane. If NetProwler has not observed any conversations of that type, the list will be empty.

In the Conversations list in the Monitor pane, Server Address always refers to the system being monitored by NetProwler and Client Address refers to the other system, regardless of which system initiated the session.

2. Double-click a conversation to view.

   The conversation appears in a separate window. If it is a common conversation type, you will see the conversation as it would appear to a session user.

   In the **Monitor** pane, the **Capture** column value for that conversation row changes to **Display** to indicate that the conversation is currently being displayed.

Terminating Conversations

A security administrator can use NetProwler not only to discover what kinds of network conversations are occurring, but to terminate any of these conversations if they appear to be unauthorized network sessions. With this capability, it is possible to monitor *and* secure a network dynamically.

To terminate a current network conversation:

1. In the **Monitor** tree, expand **Conversations** (if necessary) and select a conversation type (**Generic** to see anything not in one of the predefined categories).

   The list of current conversations of that type appears in the Monitor pane. If NetProwler has not observed any conversations of that type, the list will be empty.

NOTE

In the Conversations list in the Monitor pane, Server Address always refers to the system being monitored by NetProwler and Client Address refers to the other system, regardless of which system initiated the session.

2. Select a conversation to terminate.
3. Click **Terminate** (in the lower right of the **Monitor** pane).

   The specified network conversation is terminated. NetProwler does this by sending a spoofed RST packet, which causes the session to be closed.

Capturing Conversations

In addition to being able to monitor and terminate network conversations, NetProwler also lets you capture an active conversation and save it in a file for closer examination at a later time, or for prosecution purposes.

As with viewing a network conversation, common types of connections to systems monitored by NetProwler can be captured and replayed in a mode that shows what the user who makes the connection sees. For example, a captured telnet session will consist of a shell prompt and shell command followed by the telnet server response, then the next command, and so forth. Other types of conversations are captured packet by packet and shown in both ASCII text and hex.

To capture a network conversation:

1. In the **Monitor** tree, expand **Conversations** (if necessary) and select a conversation type (**Generic** to see anything not in one of the predefined categories).

   The list of current conversations of that type appears in the Monitor pane. If NetProwler has not observed any conversations of that type, the list will be empty.

NOTE

In the Conversations list in the Monitor pane, Server Address always refers to the system being monitored by NetProwler and Client Address refers to the other system, regardless of which system initiated the session.

2. Select a conversation to capture.
3. Click **Start Session Capture** (at the bottom of the **Monitor** pane).

The Capture Session To File dialog box appears.

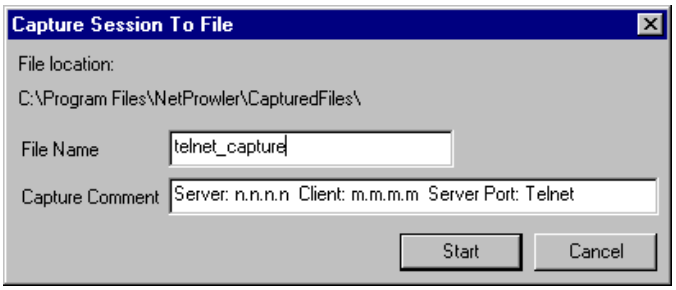


Figure 9-2: Capture Session To File dialog box

4. Type the name for the file where the captured session will be stored.
5. Type a comment to be stored along with this capture session.

   By default, the server address, client address, and application port are inserted as the capture comment.
6. Click **Start**.

   NetProwler begins capturing the session. In the Monitor pane, the Capture column value for that conversation row changes to Conversation_File to indicate that the conversation is being saved in a file.
7. To stop capturing that network conversation, click the conversation in the **Monitor** pane, and then click **Stop Session Capture**.

   In the Monitor pane, the Capture column value for that conversation row changes to Off.

Viewing Captured Conversations

Once you have captured a network conversation (see *Capturing Conversations* earlier in this chapter for more information), it is saved in a file, and can be displayed at any time. By default, captured conversations are saved in the CapturedFiles folder inside the main NetProwler program directory (by default, C:\Program Files\NetProwler).

To a captured conversation:

1. In the **Monitor** tree, expand **Conversations** (if necessary) and then click **Captured Conversations**.

   Any captured conversations appear in a list in the **Monitor** pane.

NOTE

In the Captured Conversations list in the Monitor pane, Server Address always refers to the system being monitored by NetProwler and Client Address refers to the other system, regardless of which system initiated the session.

2. Double-click any conversation row in the **Monitor** pane to see the contents of that captured conversation file.

To view a captured conversation in any folder on a local or network disk:

1. In the NetProwler Tool Bar, click **Replay**.
2. Use the **Windows Open** dialog box to select a conversation file.
3. Click **Open** to see the contents of that captured conversation file.

Chapter 10

Generating and Viewing Reports

Overview

NetProwler lets you generate four types of reports, including three types of scheduled reports, which are periodic snapshots of your network security, and a query report, which allows you to pinpoint particular types of problems. Reports can give you very detailed information about network problems detected by NetProwler, or they can give you summaries of that information, summing up network security and assessing the possible cost of unauthorized or malicious network activity.

Reports are generated from NetProwler alerts, which includes all the types of information gathered by NetProwler, such as attack alarms, conversations starts and stops, consistency problems, and system accesses. You can create as many reports as you need to examine any one of these types of problems, and even narrow your focus to particular machines on your network or particular intruder systems.

NetProwler reports can be generated in HTML format, in tab-delimited or comma-delimited format (for analysis using a popular report writers, spreadsheets, or databases), or as e-mail

messages sent to users. You can also run shell commands when reports are generated to copy reports to particular folders, launch custom security applications, and so forth.

In this chapter, you will learn how to:

- Schedule several types of NetProwler reports.
- Modify scheduled reports.
- Generate a report by querying the Alerts database.
- View and delete reports generated by NetProwler.

Scheduling Reports

Executive Summary

Executive Summary reports present a high-level overview of the number and risk level of attacks seen during a given time period, including a comparison of attacks seen and attacks expected. Executive Summary reports are a good way to take periodic snapshots of your overall network security.

To schedule an Executive Summary report:

1. In the **Configure** tree, click **Reports**.
2. Click **Add New** (below the reports list).

The Schedule Reports Entry dialog box appears.

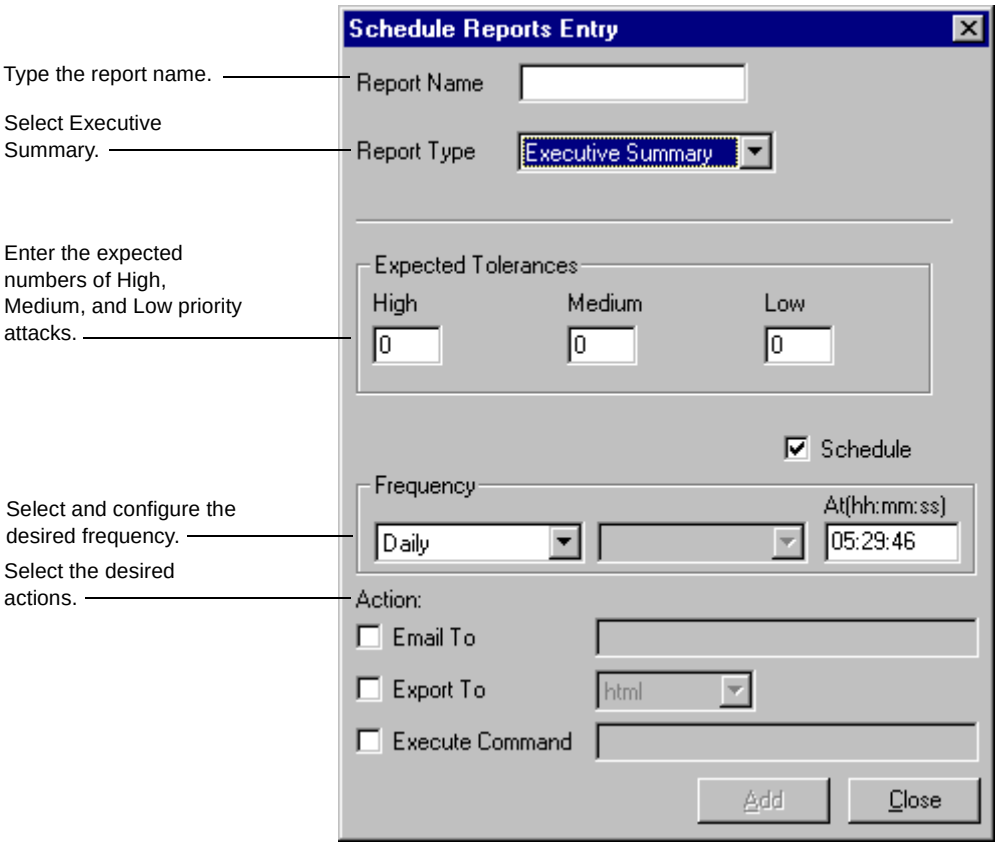


Figure 10-1: The Schedule Reports Entry dialog box.

3. Type a report name in the **Report Name** text box.
4. Choose **Executive Summary** from the **Report Type** drop-down list.
5. Type percentage values for **High**, **Medium**, and **Low** in the **Expected Tolerances** box.

   These tolerances are percentages of acceptable attacks for each category. For example, typing 10 for low would indicate that you expect 10% or less of all attacks for the period of the report to be low priority attacks.

6. Choose how often you want this report to be generated by specifying **Frequency** options.

   For Executive Summary reports, you can choose Daily, Weekly, or Monthly. For Daily reports, you must also specify a time (using a 24-hour clock). Weekly reports require a day of the week and a time. Monthly reports require a date (1-31) and a time.

NOTE

The Schedule check box must be selected (as it is by default) in order for this report to be generated at the times you specify.

7. Specify an action to perform when the report is generated. You can choose from:

   - **Email To.** Type an e-mail address in the text box next to this option. If you want multiple people to receive this report, specify a group or distribution list.
   - **Export To.** Executive Summary reports can only be exported to HTML files.
   - **Execute Command.** Type the command you want to run in the text box next to this option.

8. Click **Add** to add this report to the Reports list.
9. To add another report, repeat **Steps 2–8**.
10. Click **Close** to close the **Schedule Reports Entry** dialog box.
11. Click **Apply** to save and apply your changes.

Cost Analysis

Cost Analysis reports use figures you provide about the value of particular servers to estimate how much the attacks seen during a given time period cost you. Cost analysis reports can also help illustrate the value of implementing good network security practices.

To schedule a Cost Analysis report:

1. In the **Configure** tree, click **Reports**.
2. Click **Add New** (below the reports list).

The Schedule Reports Entry dialog box appears.

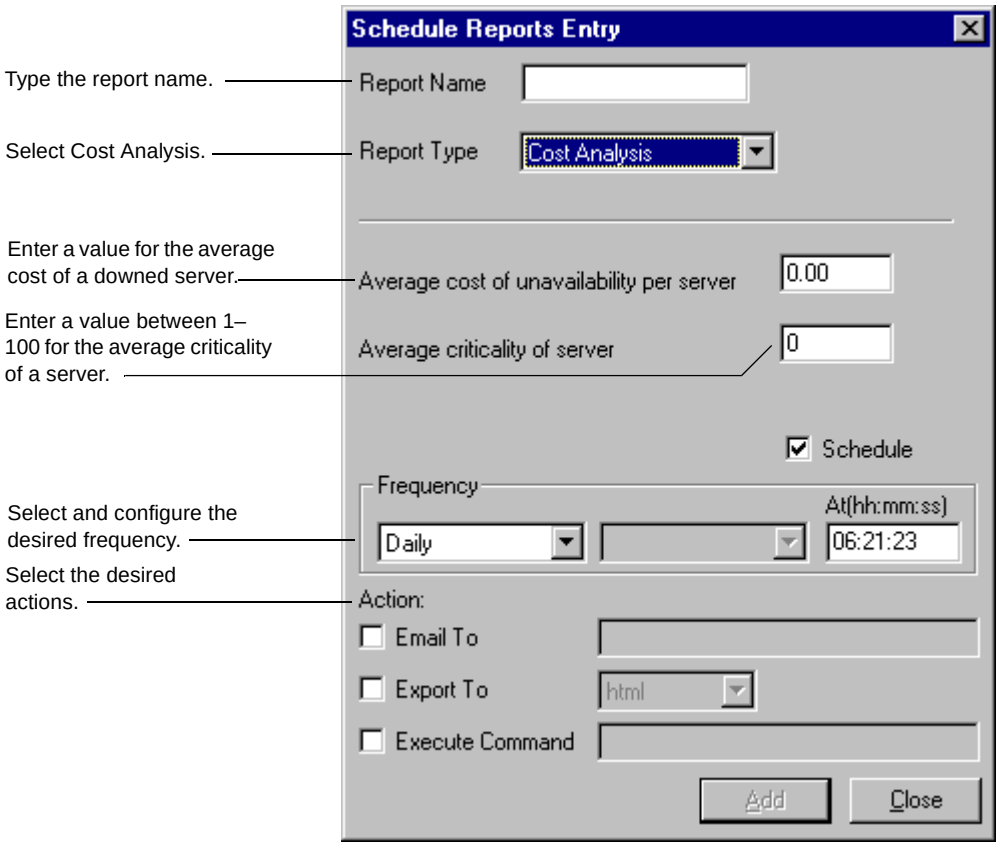


Figure 10-2: The Schedule Reports Entry dialog box.

3. Type a report name in the **Report Name** text box.
4. Choose **Cost Analysis** from the **Report Type** drop-down list.
5. Type a cost value in the **Average cost of unavailability per server** text box.

   This is your estimate of how much it would cost your organization not to be able to access each server for whatever duration you specify under **Frequency** in this dialog box.

6. Type a value (1-100) in the **Average criticality of server** text box.

   This is your estimate of the average importance of the servers covered by that particular installation of NetProwler (or in other words, on that segment of the network, since NetProwler can only look at one network segment).

7. Choose how often you want this report to be generated by specifying **Frequency** options.

   For Cost Analysis reports, you can choose **Daily**, **Weekly**, or **Monthly**. For Daily reports, you must also specify a time (using a 24-hour clock). Weekly reports require a day of the week and a time. Monthly reports require a date (1-31) and a time.

NOTE

The Schedule check box must be selected (as it is by default) in order for this report to be generated at the times you specify.

8. Specify an action to perform when the report is generated. You can choose from:

   - **Email To.** Type an e-mail address in the text box next to this option. If you want multiple people to receive this report, specify a group or distribution list.
   - **Export To.** Executive Summary reports can only be exported to HTML files.
   - **Execute Command.** Type the command you want to run in the text box next to this option.

9. Click **Add** to add this report to the Reports list.
10. To add another report, repeat **Steps 2-9**.
11. Click **Close** to close the **Schedule Reports Entry** dialog box.
12. Click **Apply** to save and apply your changes.

Attack Details

Attack Details reports show an attack history during a given time period, detailing particular types of attacks, when the attacks took place, and which machines were attacked. Attack Details reports are best for analyzing which machines on a network are most vulnerable, assessing attack patterns, and building a plan for improving network security.

To schedule an Attack Details report:

1. In the **Configure** tree, click **Reports**.
2. Click **Add New** (below the reports list).

The Schedule Reports Entry dialog box appears.

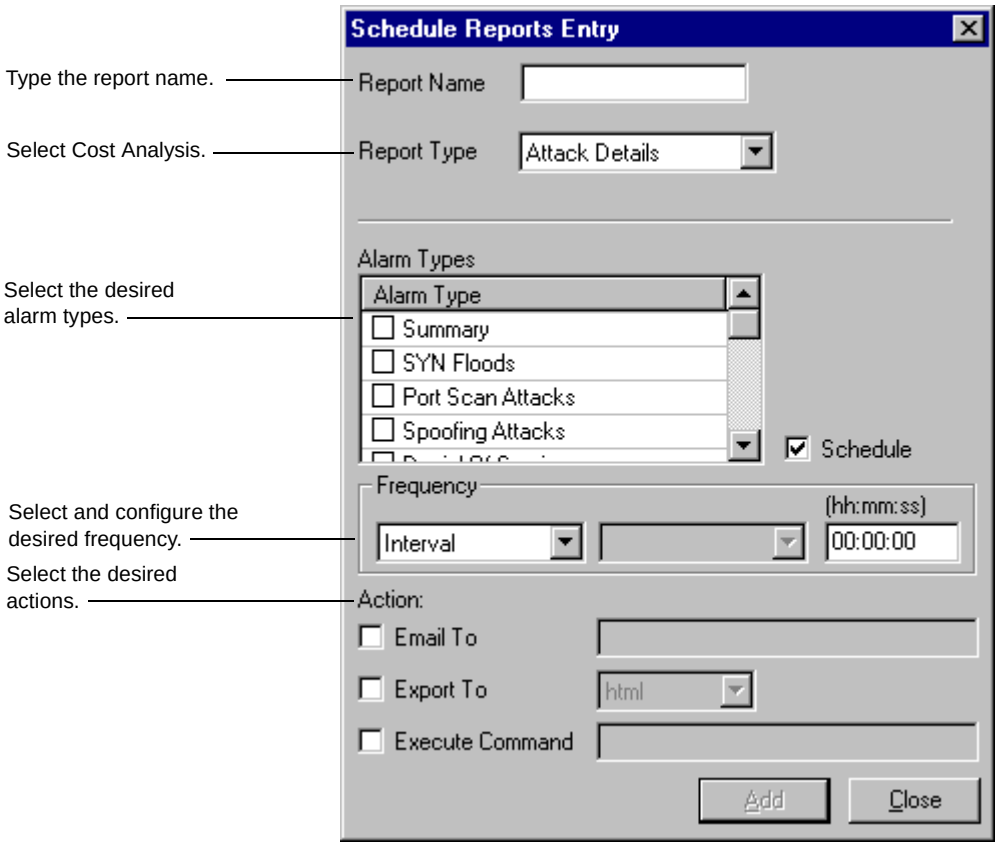


Figure 10-3: The Schedule Reports Entry dialog box.

3. Type a report name in the **Report Name** text box.
4. Choose **Attack Details** from the **Report Type** drop-down list.
5. Select the types of alarms you want to have included in this report by placing checks next to items in the **Alarm Types** list.
6. Choose how often you want this report to be generated by specifying **Frequency** options.

For Attack Details reports, you can choose Interval, Hourly, Daily, Weekly, or Monthly. Interval generates a report every x hours:minutes:seconds (where x is the length of time between reports). Hourly generates a report at the time specified each hour. For example specify 00:25:00 to have reports generated at 11:25, 12:25, 1:25, etc. For Daily reports, you must also specify a time (using a 24-hour clock). Weekly reports require a day of the week and a time. Monthly reports require a date (1-31) and a time.

NOTE

The Schedule check box must be selected (as it is by default) in order for this report to be generated at the times you specify.

7. Specify an action to perform when the report is generated. You can choose from:

   - **Email To.** Type an e-mail address in the text box next to this option. If you want multiple people to receive this report, specify a group or distribution list.

   - **Export To.** Attack Details reports can be exported to HTML files, comma-delimited files (CSV), and tab-delimited files (TSV).

   - **Execute Command.** Type the command you want to run in the text box next to this option.

8. Click **Add** to add this report to the Reports list.
9. To add another report, repeat **Steps 2–8**.
10. Click **Close** to close the **Schedule Reports Entry** dialog box.
11. Click **Apply** to save and apply your changes.

Modifying Scheduled Reports

In the Configure pane you can view a list of scheduled reports, modify existing report settings, delete scheduled reports, or turn off scheduled reports without deleting them.

Viewing and Modifying Currently Scheduled Reports

Once you have scheduled a report, you may want to keep the report but change some of it settings. For example, you may want to reschedule the report for a different time or expand the report information to include more details.

To view a list of currently scheduled reports:

1. In the **Configure** tree, click **Reports**.

   The reports list appears to the right of the tree in the Configure pane, and includes the name, type, and frequency of the report, and whether the report is currently scheduled to run (see *Turning Off Scheduled Reports* later in this chapter for more information).

To modify a currently scheduled report:

1. In the **Configure** tree, click **Reports**.
2. Double-click any of the reports in the list.
3. Follow the steps for that particular type of report under *Scheduling Reports* earlier in this chapter to make any modifications (except that the **Add** button is now changed to **Update**).
4. Click **Apply** (to the lower right of the Reports list).

Deleting a Scheduled Report

You can delete reports you are sure you never want to use again.

To permanently remove a report:

1. In the **Configure** tree, click **Reports**.

   The reports list appears to the right of the tree in the **Configure** pane.
2. Select a report in the list.
3. Click **Delete** below the reports list.
4. Click **Apply** (to the lower right of the Reports list).

Turning Off Scheduled Reports

You can turn off scheduling for a particular report without removing it from your reports list, in cases where you expect to use that report configuration at a later time.

To stop a report from being generated without deleting it from your report list:

1. In the **Configure** tree, click **Reports**.

   The reports list appears to the right of the tree in the Configure pane.
2. Double-click any of the reports in the list.
3. Remove the check in the **Scheduled** check box.
4. Click **Update**.
5. Click **Apply** (to the lower right of the Reports list).

Viewing Reports

Scheduled reports that are generated in HTML format can be shown in the Monitor pane. Other report types (comma-delimited and tab-delimited) can be opened in other applications, but cannot be opened directly from NetProwler. To delete reports, use the Windows Explorer.

Viewing HTML Reports

You can open HTML reports from within NetProwler.

To view an HTML report:

1. In the **Monitor** tree, expand **Reports** and click **Generated Reports**.

   A list of reports appears in the Monitor pane.

2. Double-click any report in the list to open it in your default browser.

You must have a properly configured web browser associated with HTML files to use this feature. If you try to open a report in NetProwler and see a Windows dialog box asking you what application you want to open the file into, then you need to specify an existing browser or install a browser if one is not installed on that system.

The contents of the report depend on the type of report generated. However, all reports have a contents listing at the top made up of links to report sections. Click any of the content's links to see sections of the report.

Viewing CSV and TSV Reports

Comma-delimited (CSV) and tab-delimited (TSV) reports generated by NetProwler can be viewed only in other applications, such as spreadsheets or databases. These reports are saved in the ReportFiles folder, which is inside the NetProwler application folder (if you chose the default path during setup, this is **C:\Program Files\NetProwler**).

Deleting Reports

Use the Windows Explorer utility to delete reports. Reports are saved in the ReportFiles folder, which is inside the NetProwler application folder (if you chose the default path during setup, this is **C:\Program Files\NetProwler\ReportFiles**).

Generating User-defined Reports

While scheduled reports are a good way to generate periodic snapshots of some aspect of network security, the Query feature lets you pinpoint any type of information stored by NetProwler in the Alerts database, which includes every security incident NetProwler has detected (unless you have at some point purged the Alerts database). The following instructions describe how to search the Alerts database for the information you want.

To query the Alerts database:

1. In the **Monitor** tree, expand **Reports** and click **Query.**

   Query options appear in the **Monitor** pane.

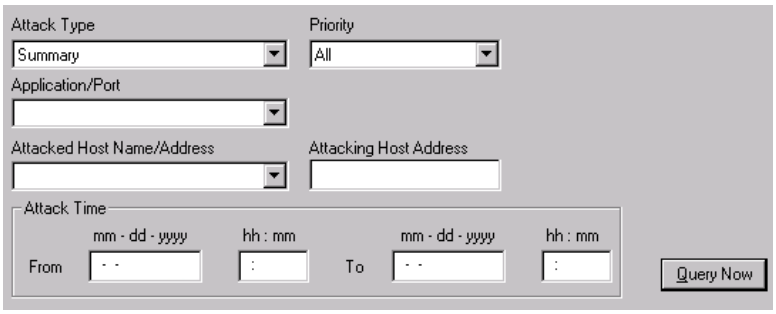


Figure 10-4: Query Options

2. Specify what kinds of alerts you want to find.

The table below describes the available options. You can leave an option blank to search for all items of that type.

Option	Description
Alarm Type	Use this option to narrow your search to a particular type of security problem detected by NetProwler. Options include a summary (or all attacks), common attacks, system accesses, sessions (conversations), consistency problems, and ASD alarms.
Application	Use this option to narrow your search to a particular application that was the focus of an attack. For example, you could specify that you only want to see information about attacks using the FTP protocol.
Server Name	Use this option to narrow your search to one of the systems being monitored by NetProwler (i.e., one of the systems in the Address Book).
Client IP Address	Use this option to narrow your search to a particular attacking or connected system. For example, if a system not in the Address Book made several telnet connections to systems in the Address Book, you could use this option to focus on all the connections by that outside system.
Priority	Use this option to select the desired priority level. Select All to select all priority levels.
Duration	Use this option to narrow your search to attacks that took place within a certain time frame.

Table 10-1: Query Options

3. Click **Query Now** to begin your search.

   The query results appear as a list of alerts that match your query criteria. Each row in the list contains one attack.

   You can save your query results as a comma-delimited file for further analysis. For more information about how to save a report in one of these formats, see *Saving a User-defined Report* on page 10.17.

4. To generate a new query, click **New Query** (in the lower right of the Monitor pane) and repeat **Steps 1–3**.

Saving a User-defined Report

Query reports can be saved as comma-delimited files for further analysis using a spreadsheet or database application.

To save the results of a query:

1. If you have not already done so, execute a query.

   For instructions on how to execute a query, see *Generating User-defined Reports* on page 10.15.

2. Click **Save** (in the lower right of the **Monitor** pane).

3. Specify a file name, file location, and file type using the Windows **Save As** dialog box.

4. Click **Save**.

Appendices

Reference Data

Appendix A: Getting Help with NetProwler

Appendix B: Optimizing NetProwler's Performance

Appendix C: Attack Signature Descriptions

Getting Help

Overview

AXENT Technologies provides the following support services:

- Online Help
- User Manuals
- Release Notes
- AXENT Online
- Training
- Technical Support
- AXENT Consulting Services
- Links to Other Security Resources

Online Help

Online Help contains conceptual and "how-to" information about the software, and can be accessed from the Help menu, Toolbar, or by pressing F1. There are three ways to find topics in a help file: Contents (similar to the table of contents in a book), Index (a searchable alphabetical list of program terms and synonyms), and Search (a searchable alphabetical list of every word in the help file). See *Figure A-1: Online Help*, below.

Choose the Contents tab to search by topic. Choose the Index or Search tabs to search by keyword.

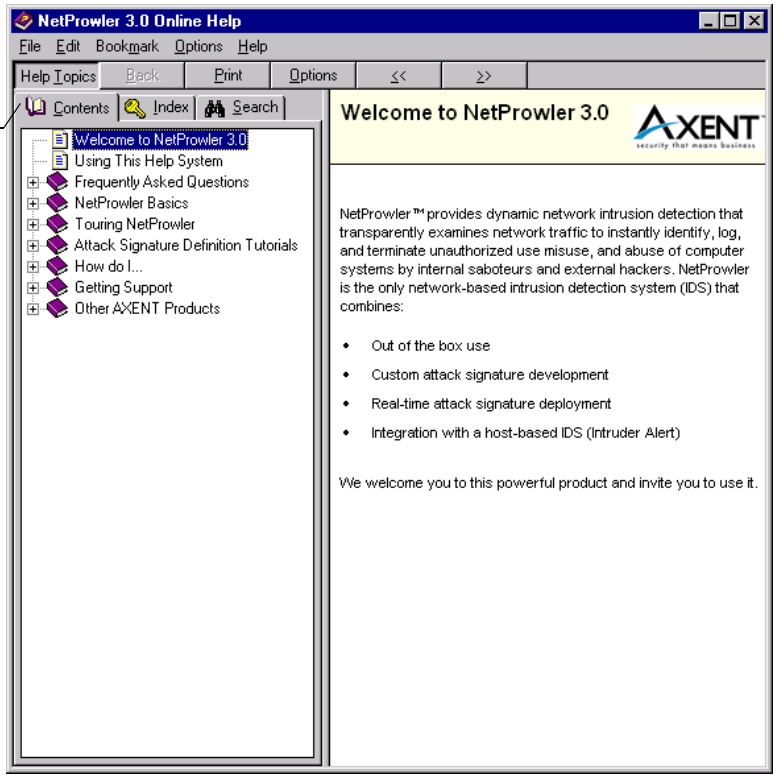

NetProwler 3.0 Online Help
File Edit Bookmark Options Help
Help Topics Back Print Options << >>
Contents Index Search
Welcome to NetProwler 3.0
Using This Help System
Frequently Asked Questions
NetProwler Basics
Touring NetProwler
Attack Signature Definition Tutorials
How do I...
Getting Support
Other AXENT Products
Welcome to NetProwler 3.0
AXENT
NetProwler™ provides dynamic network intrusion detection that transparently examines network traffic to instantly identify, log, and terminate unauthorized use misuse, and abuse of computer systems by internal saboteurs and external hackers. NetProwler is the only network-based intrusion detection system (IDS) that combines:
Out of the box use
Custom attack signature development
Real-time attack signature deployment
Integration with a host-based IDS (Intruder Alert)
We welcome you to this powerful product and invite you to use it.

Figure A-1: Online Help

User and Installation Manuals

Users should read the User and Installation manuals and become familiar with their content before contacting customer support.

User manuals contain theoretical, conceptual, and instructional information about the software. In AXENT manuals, you will find:

- Conceptual information.
- Pre-installation, installation, and post-installation information.
- Instructions for using the software.
- Configuration and optimization information.
- Sources for additional help, including online resources and customer support.

Online user manuals come on the software CD in Adobe® Acrobat™ format.

Release Notes

Release notes introduce the software and describe what is new in the latest release. Users should read the release notes before installing the software.

A copy of the release notes accompanies the manual and software CD-ROM. Release notes are also available on the AXENT web site at *http://www.axent.com*.

Online Support Services

AXENT provides many types of support services that can be accessed on the AXENT web site at *Http://www.axent.com*

AXENT's online support services include:

Technical Support Policies and Procedures

The Policies and Procedures page describes licensing procedures, incident reporting procedures, escalation procedures, product support policies, year 2000 compliances, and Defender support.

Notification List Services

Customer notification mailings provide information about new product upgrades, releases, tune-up packs, and company updates via e-mail. AXENT customers may subscribe to this service and stay informed on what is happening at AXENT.

Global Online Incident

Use the Global Online Incident Form to submit OmniGuard service requests electronically to AXENT's World Wide Support Centers.

Product Upgrade Requests

Use the OmniGuard Upgrade Request Form to order product upgrades for any OmniGuard product.

License Key Requests

Use the OmniGuard License Key Request Form to request license keys for NetProwler.

Customer Satisfaction Assistant

Use the Customer Satisfaction Assistant Survey Form at to submit your comments electronically to the World Wide Support Centers to help us improve our service.

Security Forum

The Security Forum offers information security professionals a place to discuss and resolve information system security problems. AXENT engineers and consultants maintain this site and are available to answer questions about technical issues or offer tips and techniques.

Information Security SWAT Web Site

The SWAT web site provides security solutions and strategies related to the industry's most common security threats. NetProwler users can also find new attack signatures developed by AXENT at the site.

Training

AXENT offers training seminars on a regular basis. We invite you to attend these training courses at one of our training facilities. AXENT's training headquarters is located in Waltham, Massachusetts, U.S.A., but AXENT also offers training in several major U.S. cities. AXENT can also arrange on-site training for your organization if the appropriate training environment is available. The following is a list of training seminars we offer.

- Enterprise Security Manager2 Days
- Intruder Alert 2 Days
- NetProwler 2 Days
- NetRecon 1 Day
- Raptor Firewall Fundamentals 2 Days
- Raptor Firewall Advanced 2 Days
- Security Briefcase (3 topics) 2 Days
  - Defender
  - PowerVPN
  - PCShield

All courses are accredited by the EDPAA. You can earn 4 CPEs for a half-day workshop, 8 CPEs for a 1-day workshop, 12 CPEs for a 1½-day workshop, and 16 CPEs for a 2-day workshop.

You can register for AXENT training courses on our web site at:

http://www.axent.com

For more information on AXENT training or registration questions, contact registration at:

Phone: (781) 530-2267

Fax: (781) 530-2207

E-mail training@axent.com

Tradeshows

AXENT actively participates in information security tradeshows throughout the world. At tradeshows, you will learn about AXENT's latest product and service offerings. For up-to-date scheduling information, see us on our web site at *http://www.axent.com*.

Technical Support

AXENT's Technical Support group is a team of skilled Product Champions that provide platform-specific information about AXENT products. Our staff has in-depth expertise in both client / server computing and information security technology. Customer Support hours are from 6:00 AM to 6:00 PM MST Monday through Friday.

Before Contacting Technical Support

For help using a Intruder Alert, read the user manuals and product release notes. If you are unable to find a solution, complete the following steps before calling Technical Support:

1. Become an authorized contact with your security manager.
2. See if the solution to your problem can be found on AXENT's web pages.
3. Find out if a Tune-up pack or upgrade is available.
4. Log your request using AXENT's Global On-Line Incident form available from the AXENT web site at *http://www.axent.com*
5. Gather the relevant information described in Tables A-1 and A-2.
6. If you call support, be at the computer, so our Product Champions can talk you through the steps needed to correct the problem.

Console Information

Information	Source
Machine Type:	Get from the Windows "System Properties" dialog.
OS Level:	Get from the Windows "System Properties" dialog.
Version:	Get from the Help menu's About dialog.
Date:	Get from the Help menu's About dialog.
Service Pack	Get from the Help menu's About dialog.

Table A-1: Required GUI Information

Network Information

Information
Find out the type of network and Network Interface Card (NIC). NetProwler requires an Ethernet adapter on a 10/100MB ethernet network.

Table A-2: Required Network Information

Problem Information

Information
List all the steps needed to reproduce the problem.
Describe the symptoms of the problem.
Note the exact wording of any error messages (every character counts).
Print, fax, or e-mail copies of the install.log and crash.dat files from the NetProwler directory and any Dr. Watson report information.
Provide any other relevant information about the problem.

Table A-3: Required Problem Information

Contacting Technical Support

To contact AXENT's technical support:

United States

U.S. Support Center:	**(801) 227-3700**
Fax:	**(801) 227-3788**
E-mail:	**support@axent.com**

Europe

European Support Center:)	**+44 1372 214321**
FAX:	**+44 1372 214341**
E-mail:	**support@axent.co.uk**

Licensing

Licensing:	**(888) 584-3925**
E-mail	**License@axent.com**

World Wide Web site

World Wide Web:	http://www.axent.com

Anonymous FTP

FTP:	www.axent.com

AXENT Consulting Services

AXENT offers both presales support services and information security consulting. AXENT's Presales Engineers provide the following free services for clients evaluating AXENT products:

- Presentations
- Free evaluations
- Technical questions prior to the sale
- Product support prior to the sale

AXENT's consulting service group, Secure Network Consulting Inc. (SNCi) is comprised of skilled professionals trained in both client/server computing and information security technology. SNCi provides a mature range of consulting services. Available services include:

- Information Security Consulting
- Security Engineering and Systems Integration
- Executive, User, and Technical Education
- Information Security Product Development Support and Evaluation
- 10-day Diagnostic Vulnerability Assessment
- Firewall Installation
- Vulnerability Assessment Subscription Service

Contact the SNCi for pricing information at:

Phone:	(210) 892-7624
Fax:	(210) 892-7625
E-mail:	info@snc-inc.com

Links to Other Security Resources

AXENT's web site provides links to more than 40 other security resources, such as:

- Security organizations
- Security related news groups
- Emergency response teams
- Journals and newsletters

For links to these information resources, please see AXENT's web site at *http://www.axent.com/support/secres/default.htm*.

Appendix B

Optimizing NetProwler's Performance

Overview

This appendix describes how to evaluate and improve NetProwler's performance. Several factors may affect NetProwler's performance:

- The speed of the network
- The amount of network traffic
- The system's hardware configuration (i.e. processor, memory, etc.)
- The number of hosts being monitored
- The number and complexity of applied attack signatures

The following section, *Monitoring NetProwler's Performance*, describes how to use the Monitor pane to display frame statistics and protocol distribution information. The *Improving NetProwler's Performance* section offers tips on how to improve NetProwler's performance.

Monitoring NetProwler's Performance

You can monitor NetProwler's performance to determine:

- The amount of traffic on the network segment
- The kind of traffic monitored
- The number of frames processed
- The number of frames dropped

To Monitor NetProwler's Performance:

1. In the **Monitor** tree, click the **Counters** branch.

   The Monitor pane displays the Frame Statistics and Protocol Distribution information.

The Monitor pane displays the number of frames processed, the number of frames dropped, the time that NetProwler started monitoring, and the types of network traffic monitored.

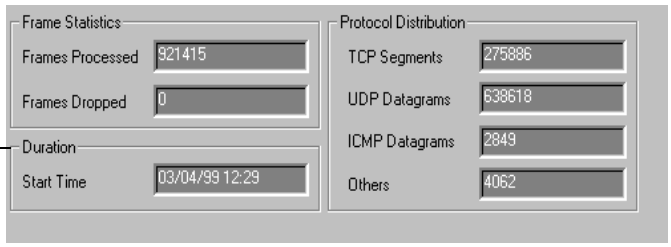


Figure B-1: Frame Statistics and Protocol Distribution

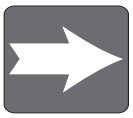
The number of frames dropped refers to network traffic that NetProwler did not monitor because it did not have enough memory or available CPU cycles to analyze the traffic. During normal network conditions, NetProwler should not drop frames. If NetProwler is dropping frames, you should increase the system memory, monitoring fewer hosts, or add an additional installation of NetProwler. As a rule of thumb, you should upgrade your system's configuration if 3 percent or more of the total frames processed are being dropped.

Improving NetProwler's Performance

To ensure optimal performance, AXENT recommends installing NetProwler on a dedicated Windows NT system. This ensures that NetProwler remains secure and has the system resources necessary to monitor network traffic on large segments. NetProwler attempts to obtain 100 percent CPU usage on the system where it is installed.

The dedicated Windows NT system requires at least a Pentium or Pentium equivalent processor with a minimum of 64 MB of ram and 50 MB of hard disk space.

If NetProwler is dropping more than three percent of the total frames, consider:



- Upgrading the CPU
- Adding more memory
- Simplifying NetProwler's configuration by monitoring fewer hosts or reducing the number of associated attack signatures.
- Purchasing an additional copy of NetProwler for the network segment and dividing the number of attack signatures and monitored hosts between the two NetProwler installations (This is known as load balancing.)

B.4 Optimizing NetProwler's Performance

Attack Signature Descriptions

Overview

Appendix C lists and describes the attack signatures contained in NetProwler. They are arranged in alphabetical order.

NetProwler's Predefined Attack Signatures

Apache_Web_Server_Denial_of_Service_Attack

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

ARP_Host_Down_Check

ARP Host Down Check

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

ASCEND_ROUTE_ASCEND_KILL

Exploit that kills Ascend Routers.

By sending a specially formatted malformed TCP packet to Ascend routers containing certain versions of the Ascend operating system, the router can be forced to cause an internal error, resulting in the router rebooting.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

BackOrifice_Detect

Attempt to detect the BackOrifice attack on the network.

BackOrifice, once installed on a system, transmits information about the machine over the network, "snooping" the screen and keyboard of the machine where it was installed. This alert detects BackOrifice communication.

Applicable Operating Systems:

- Network- or Application-based attack

Bonk_Attack

Another variation of TearDrop

Applicable Operating Systems:

- Network- or Application-based attack

Brute_Force_Login_Attempt

Detects repetitive failed login attempts on hosts.

Applicable Operating Systems:

- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

Cookie_Monster_Attack_Decode

Detects the Cookie Monster Attack.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

DIG_Attack

Detects DIG attack

The DIG attack uses DNS to obtain information about a remote network. This alert detects such probing.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

DNS_REQUEST_BROADCAST

Exploit to send DNS Request to broadcast IP Address

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

DNS_Zone_Transfer_Decode

Detect DNS Zone Transfer packets on the network

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

Duplicate_IP_Address_Detection

Multiple hosts with the same IP address detected on the network.

Only one machine on a network should send packets with a specific IP address. If a second machine on the network starts to send packets claiming to have the same source address, a network problem has occurred. A machine on the network may be misconfigured to have the same IP address as another machine, causing network conflicts. The other possibility is that a machine on the network may be sending out IP packets with a forged source address.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS

- HP / UX
- AIX
- Linux

Echo_Chargen_loop_Attack

Attack using Echo and Chargen as the Destination and Source Ports respectively.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

E-mail_From_Decode

Records the sender of an SMTP e-mail message.

Applicable Operating Systems:

- Windows NT
- Windows 95
- Solaris
- Sun OS
- HP/UX
- AIX

E-mail_To_Decode

Records the recipient of an SMTP e-mail message.

Applicable Operating Systems:

- Windows NT
- Windows 95
- Solaris
- Sun OS
- HP/UX
- AIX

Finger_User_Decode

Decodes the user being fingered.

Applicable Operating Systems:

- Windows NT
- Windows 95
- Solaris
- Sun OS
- HP/UX
- AIX

FTP_CWD_Vulnerability

Attackers who can access FTP on the target host to transfer files to which they would normally be denied access

Applicable Operating Systems:

- Windows NT
- Windows 95
- UNIX

- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

FTP_Get_File_Decode

Records the name of the file being retrieved via FTP.

Applicable Operating Systems:

- Windows NT
- Windows 95
- Solaris
- Sun OS
- HP/UX
- AIX

FTP_MKDIR_Decode

Discovers all new directories that are created by a user through FTP

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

FTP_Password_Decode

Discovers the FTP password.

Applicable Operating Systems:

- Windows NT
- Windows 95
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX

FTP_PUT_Decode

Decodes FTP file transfers to a destination host

Applicable Operating Systems:

- Windows NT
- Windows 95
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

FTP_RMDIR_Decode

Decodes all directory removals that are done on a target host using FTP

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

FTP_Root_User_Access_Decode

Discovers a user trying to login to a target host as root using FTP

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

FTP_Scan

An FTP vulnerability exploited to scan victim's port numbers

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

FTP_SITE_EXEC_Vulnerability

Discovers a site exec command being used through FTP

Certain versions of wu-ftpd allow using a site exec command to execute commands on a remote machine. By providing a pathname with certain characteristics, a remote user can execute arbitrary commands on the FTP server.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

FTP_SITE_Vulnerability

Discovers the use of the site command through FTP

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

FTP_USER_Decode

Discovers the FTP user name being used to transfer files across the network through FTP

FTP allows users to transfer files between machines. Username decoding discovers the name of the account being used to transfer files across the network.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

FTP_Arg_Core_Dump_Decode

Detects continous attempts to login to the FTP server which may crash the server.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

HP_UX_NETTUNE_Attack

Nettune utility by default runs in SETUID root therefore any user can change a vast number of network related parameters.

The Nettune utility by default runs in SETUID root. Therefore any user can change a vast number of network related parameter resulting in an attack.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

HP_UX_PPL_EXPLOIT_Attack

The PPL implementation of HP/UX, HP's version of SLIP allows to modify the /.rhosts file.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

HPUX_RemoteWatch_Vulnerability

Watches accesses to the RemoteWatch service on HP/UX

Certain versions of HP/UX that come with the RemoteWatch package installed have a vulnerability which allows a remote attacker to execute arbitrary commands through the RemoteWatch service on the target machine. This vulnerability check will watch accesses to the RemoteWatch service and determine if these accesses are attempting to exploit his vulnerability.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris

- Sun OS
- HP / UX
- AIX
- Linux

HTTP_Campas_CGI_Vulnerability

This exploit allows a remote attacker to execute commands on the Web server machine as the user the httpd process is running as.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

HTTP_Convert_CGI_BIN_Vulnerability

This exploit allows a remote attacker to execute commands on the Web server machine as the user the httpd process is running as.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX

- AIX
- Linux

HTTP_Glimpse_Vulnerability

This exploit allows a remote attacker to execute commands on the Web server machine as the user the httpd process is running as.

This check will recognize an attack against the glimpse cgi-bin script present with certain httpd Web servers. This exploit allows a remote attacker to execute commands on the Web server machine as the user account accessed by the httpd process itself.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

HTTP_Java_Decode

Recognizes a web browser's attempt to obtain a file that contains Java bytecode

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS

- HP / UX
- AIX
- Linux

HTTP_NPH_TEST_Vulnerability

Identifies an attack on the cgi-bin nph-test-cgi script (that is installed by default with certain versions of Apache and NCSA Web servers)

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

HTTP_PHF_CGI_Vulnerability

Certain versions of NCSA / Apache Web servers that have the cgi-bin script PHF pre-installed, have a vulnerability that allows any Web user access to the machine(s)

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX

- AIX
- Linux

HTTP_SGI_Wrap_Vulnerability

Recognizes an attack on the wrap cgi-bin script that is part of IRIX 6.2's WWW HTTP server

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

HTTP_TEST_Vulnerability

Recognizes an attack that attempts to obtain information on directory above the Web servers's root

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

HTTP_View_Source_Script_Vulnerability

Recognizes an attack on the view-source cgi-bin script included in SCO Skunkware CD-ROM distributions and other httpd servers

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

HTTP_BAT_FILE_EXEC

""".bat"" files can be downloaded and executed without users permission when the user accesses a web-page that has these files embedded

This alert detects attempts to execute an MS-Dos batch file via HTTP.

Applicable Operating Systems:

- Network- or Application-based attack

HTTP_COUNT_CGI_DECODE

Some versions of cgi-bin program are affected by this attack.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX

- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

HTTP_ETC_PASSWD_DECODE

Detect attempt to access /etc/passwd file using HTTP.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

HTTP_EXEC_ISP_FILE

""".isp"" files can be downloaded and executed without users permission when the user accesses a web-page which has this type of file embedded in it.

Applicable Operating Systems:

- Network- or Application-based attack

HTTP_UPLOADER_DECODE

Detect execution of uploader on a website

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

HTTP_WIN_C_SAMPLE_DECODE_ASD

Detecting Win-C-Sample.exe attack on O'Reilly web-servers

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

ICMP_Dst_Proto_Unreachable_Decode

Packets which have the destination unreachable code set due to unreachable protocol.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

ICMP_Redirect_Host_Redirect_Message

Icmp Host Redirect Message

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

ICMP_Redirect_Net_Redirect_Message

Icmp Net Redirect Message

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

ICMP_Redirect_Packet

An ICMP redirect packet can be sent by the attacker to redirect all packets to himself.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

ICMP_Redirect_TOS_Host_Redirect_Message

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

ICMP_Redirect_TOS_Net_Redirect_Message

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

ICMP_SMURF

A broadcast ICMP-echo packet can flood the network (Denial-Of-Service).

The Smurf attack uses ICMP to send a broadcast ping. This traffic and that of the hosts that respond (all of them) can quickly increase network congestion, preventing normal network traffic.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

IDENT_Newline_Vulnerability

If the response on Ident port contains newlines, the response may be improperly parsed, allowing the remote user to execute commands on the host machine.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

IDENT_User_Decode

Recognizes attempt to use the Ident port for identifying a user account

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

IMAP_Username_Password_Decode

Decodes Internet Message Access Protocol (IMAP) username and password.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

INVALID_TCP_FRAME_DETECT

Detect Invalid TCP Frames on the network

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

INVALID_TTL_DECODE

Detects packet with invalid IP TTL.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

IP_Options_Loose_Source_Routing_Decode

Detect Loose Source Routing Enabled in IP Packet

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

IP_Options_Record_Route_Decode

Detect IP Packet with Record Route Options Enabled

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

IP_Options_Security_Enabled_Decode

Detect IP Packet with Security Option Enabled

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

IP_Options_Strict_Source_Routing_Decode

Detect Loose Source Routing Enabled in IP Packet

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

IP_Options_TimeStamp_Decode

Detect Packet with IP options TimeStamp enabled

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

IP_Unknown_Protocol

Recognizes unknown values used in the protocol field of the IP header

A standard IP packet contains an 8-bit protocol field. Common values for this field include 6 (TCP), 17 (UDP), and 1 (ICMP). Attackers sometimes use a non-standard value for this field in order to exchange data between machines without logging mechanisms detecting the data that is being transmitted.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

IRC_Channel_Decode

Decodes the channel joined by a user on Internet Relay Chat

- Windows NT
- Windows 95
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX

IRC_Message_Decode

Decodes a message sent by a user on Internet Relay Chat.

- Windows NT
- Windows 95
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX

IRC_Nick_Decode

Decodes changes to a user's nickname on Internet Relay Chat.

- Windows NT
- Windows 95
- UNIX
- Solaris
- Sun OS

- HP / UX
- AIX

LAND

Abnormal packet causes slowdowns.

- Windows NT
- Windows 95

LATIERRA

Variation of LAND attack for TCP - it also includes a port scan

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

LINUX_Dump_Command_Vulnerability

This vulnerability allows intruder to read any files on the system.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS

- HP / UX
- AIX
- Linux

LINUX_KBD_Denial_of_service

This vulnerability allows intruder to lock up the keyboard on the system.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

LINUX_Login_Command_Vulnerability

This vulnerability allows intruder to gain root access on the system.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

LINUX_Login_Vulnerability

This vulnerability allows intruder to gain root access on the system.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

LINUX_LOGIC_BOMB_Attack

This vulnerability allows intruder to crash the system.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

LINUX_SHADOW_FILE_Attack

This check discovers when a intruder tries to access the shadow password file on the system.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

MICRO_FRAGMENT_DETECT

Detecting malformed TCP fragments.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

MS_IE_LNK_Vulnerability

Detects attempts to execute an arbitrary program on a Windows machine that is browsing the Web using Internet Explorer 3.0/ 3.01

When loaded in IE 4.01 on both Windows 95 and Windows NT 4.0 systems, this will crash the browser. In Windows 95 this bug causes two successive illegal operations, and causes Active Destop to "lose it's settings" if being used. In Windows NT 4.0 it yields a Dr. Watson which tells you that IEXPLORE.EXE caused a stack overflow, and causes Active Desktop to "lose it's settings" if being used. The "data" attribute of the "object" tag is used to reference itself. This misuse of the object tag causes the broswer to go into a loop, and eventually crash.

Applicable Operating Systems:

- Network-or Application-based attack

MS_IE_URL_Vulnerability

Detects attempts to execute an arbitrary program on a Windows machine that is browsing the Web using Internet Explorer 3.0/ 3.01.

Applicable Operating Systems:

- Network- or Application-based attack

MS_WIN_Remote_Passwd_Access

This check will recognize an access of a PWL password cache file over a NetBIOS share.

This check will recognize an access of a PWL password cache file over a NetBIOS share. PWL cache files are weakly encrypted and accessing these files over a network can be an indication of an attacker attempting to retrieve these files, or even in legitimate cases of the original user accessing his/her own cache file, it is being sent unencrypted over the network.

Applicable Operating Systems:

- Network- or Application-based attack

MS_WIN_Remote_Registry_Access

This check will recognize an access of the registry over a NetBIOS share.

This check will recognize an access of the registry on a remote machine over a NetBIOS session. The registry can be accessed remotely either through a registry modification tool (i.e., regedit) or as an automated part of normal network activity.MS_IIS_ASP_Attack

Applicable Operating Systems:

- Network- or Application-based attack

MS_IIS_ASP_Attack

This vulnerability allows viewing the contents of an active server push URL by using the hexadecimal value '2e' instead of a '.' in the URL name.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

MS_JOLT_Attack

Jolt Attack on Windows platforms - also known as SSPing Attack.

Applicable Operating Systems:

- Network- or Application-based attack

MS_WIN_SAM_ACCESS

Attempt to access the remote Windows NT SAM.

Applicable Operating Systems:

- Network- or Application-based attack

Netscape_Cache_Cow_Attack_Decode

Attack using Netscape Browsers upto versions 4.06

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

Netscape_Son_Of_Cache_Cow

Detect Netscape Son Of Cache Cow attack

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

NewTear

This crashes various systems by sending improper fragments

Applicable Operating Systems:

- Network- or Application-based attack

NFS_EXPORT_Command_Decode

This decode detects a remote showmount.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

NNTP_Group_Decode

Decode the name of a newsgroup that a user is accessing.

Applicable operating systems:

- Windows NT
- Windows 95
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX

NNTP_Password_Decode

Decodes the NNTP (Network News Transfer Protocol) password.

Applicable operating systems:

- Windows NT
- Windows 95
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX

NNTP_Username_Decode

Decodes the NNTP (Network News Transfer Protocol) username.

Applicable operating systems:

- Windows NT
- Windows 95
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX

NT_DNS_QR_Bit_Vulnerability

ONLY APPLIES TO DNS SERVERS - The DNS server on NTcrashes on an unsolicited DNS reply

Applicable Operating Systems:

- Network- or Application-based attack

NT_IIS_Telnet_GET_Vulnerability

On NT IIS 2.0 server, HTTP GET thru a Telnet client causes a crash

Applicable Operating Systems:

- Network- or Application-based attack

NT_PortMapper_Flood

NT denial of service attack based on Port Mapper application

Applicable Operating Systems:

- Network- or Application-based attack

NT_Telnet_denial_of_service

NT-Telnet-denial-of-service (NOT FOR TELNET SERVERS)

Applicable Operating Systems:

- Network- or Application-based attack

NT_DNS_Attack

An ill-formatted DNS packet to NT machines can raise the CPU utilization to 100%.

Applicable Operating Systems:

- Network- or Application-based attack

OOB_Attack_ON_NT

A packet with the TCP URGENT flag set with no TCP data to follow crashes the NT TCPstack.

A Ping Flood is an attempt to saturate a network with packets in order to slow or stop legitimate traffic going through the network. A continuous series of ICMP Echo Requests are made to a target host on the network, which then responds with an ICMP Echo Reply. The continuing combination of requests and replies slow the network and cause legitimate traffic to continue at a significantly reduced speed or, in extreme cases, to disconnect.

Applicable Operating Systems:

- Network- or Application-based attack

PING_REPLY_FLOOD

Detects flooding the network with Ping Responses.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

POP_Password_Decode

Decodes the POP (Post Office Protocol) password.

Applicable operating systems:

- Windows NT
- Windows 95
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX

POP_Username_Decode

Decodes the POP (Post Office Protocol) username.

Applicable operating systems:

- Windows NT
- Windows 95
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX

Remote_Packet_Capture_Decode

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

RLogin_Vulnerability_Attack

Checks vulnerability of certain operating systems that allow rlogin with -froot to get root access to the machine

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

SMTP_DEBUG_Decode

Detects use of the SMTP DEBUG command (in older versions of Sendmail) that could allow an attacker to gain root access to a machine

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

SMTP_EXPN_Decode

Detects attempts to use the EXPN command which could reveal information on the users of a system

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

SMTP_Piped_Command_Vulnerability

Detects attempts to use the pipe (|) character in an e-mail that could allow Sendmail to be forced to execute a command on the remote host

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

SMTP_QMAIL_Vulnerability

This check recognizes a Denial of Service attack against a Qmail mail server caused by repeated RCPT commands to the server.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

SMTP_VRFY_Decode

Detects use of the VRFY command that could allow an attacker to gain information on the users of a system

The WIZ command in Sendmail existed to allow access to a machine under certain circumstances. It is no longer present in current versions of Sendmail, but old versions still in use may allow an attacker to gain root access to a machine by using this command.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

SMTP_WIZ_Decode

Detects use of the WIZ command that could allow root access to a machine in older versions of Sendmail

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

SunOS_UDP_Bomb

Detects a UDP packet constructed with illegal values in certain fields which may cause a crash in certain older operating systems

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

SunOS_AUDIOOCTL_KERNEL_PANIC

An exploit which causes a kernel panic on SunOS 4.0 hosts.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

SunOS_dev_nit_exploit

Recognizes use of the /dev/nit device on SunOS & Solaris that can allow monitoring of network data as well as injecting data in to a stream

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

SunOS_DF_Attack

An exploit which causes a kernel panic on SunOS 4.0 hosts.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

SunOS_Keyboard_Kernal_Panic

An exploit which causes a kernel panic on SunOS 4.0 hosts.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

SunOS_Not_On_System_Console

Discovers when a user tries to login as root when not on the system console.

Applicable Operating Systems:

- SunOS

SunOS_Ping_Crash_Attack

An exploit which causes a which causes a crash of SunOS hosts.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

SunOS_TCP_Kernal_Panic

An exploit which causes a kernel panic on SunOS 4.0 hosts.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

SunOS_TCX0_Kernal_Panic

An exploit which causes a kernel panic on SunOS 4.0 hosts.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux
-

SynDrop

A variant of Teardrop which sends 2 IP fragments on TCP protocol with offset overlapping and TCP_SYN flag set.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

Syslog_fogger

An attacker can hide his trace by filling the UNIX syslog with junk

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

TearDrop

It affects NT 4 and Win95 machines with all current patches and hotfixes by sending two UDP/IP Fragments sent with overlapping offset.

Applicable Operating Systems:

- Network- or Application-based attack

Telnet_detect

Detects Telnet client connecting to any important application port

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

Telnet_Potential_Denial_of_Service

A potential denial-of-service attack can be generated on a server supporting Telnet using this method

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS

- HP / UX
- AIX
- Linux

TFTP_GET_Vulnerability

This check watches for attempts to transfer files from a machine using the Trivial File Transfer Protocol (TFTP).

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

TFTP_PUT_Vulnerability_Attack

This check watches for attempts to transfer files from a machine using the Trivial File Transfer Protocol (TFTP).

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

TRIPWIRE_Attack

This check detects attempt by hacker to cover up his tracks.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UDP_Scan

Port scan for UDP ports

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UDP_SMURF

A UDP-echo packet sent to an IP broadcast address causes a denial of service on the network.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_Finger_Access_Decode

A finger access gets the details of all the users on the host.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_Finger_Bomb_Vulnerability

This check watches for attempts to perform a denial-of-service attack against a machine or for redirecting finger attempts across machines.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_Hosts_File_Access

Checks for attempt to access the hosts file on Unix.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_Rhost_File_Access

checks for attempt to access the rhost file on Unix.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_Home_Change_Mode_Vulnerability

Checks for attempt to set the HOME variable in Unix.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_Mail_Change_Mode_Vulnerability

Checks for attempt to set the MAIL variable in Unix.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_ADM_Messages_Attack

Discovers when a user attempts to access the /adm/messages file.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_Aliases_Dir_Attack

Discovers when a user attempts to access the /aliases directory.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_Aliases_Pag_File_Attack

Discovers when a user attempts to access the /aliases/pag file.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_Bliss_Virus_Attack

Discovers when a user attempts to infiltrate the Unix host with the ""Bliss Virus"".

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_CULOG_File_Attack

Discovers when a user attempts to access the /culog file.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_Errorlog_File

Discovers when a user attempts to access the /errorlog file.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_ETC_Exports_File_Attack

Discovers when a user attempts to access the /etc/exports file.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_ETC_Host_File_Attack

Discovers when a user attempts to access the /etc/hosts file.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_ETC_Inetd_Conf_File_Attack

Discovers when a user attempts to access the /etc/inetd.conf file.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_ETC_Utmp_File_Attack

Discovers when a user attempts to access the /etc/utmp file.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_Host_Equiv_File_Attack

Discovers when a user attempts to access the /host.equiv file.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_Loginlog_File_Attack

Discovers when a user attempts to access the /loginlog file.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_Passwd_File_Attack

Discovers when a user attempts to access the password file.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_Sulog_File_Attack

Discovers when a user attempts to access the sulog file.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_Var_Adm_Lastlog_File_Attack

Discovers when a user attempts to access the /var/adm/lastlog file.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

UNIX_XLOCK_Vulnerability

This exploit enables local users to gain root access.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

Winnuke

This exploit detects out-of-band packets on a NetBios connection.

Applicable Operating Systems:

- Network- or Application-based attack

WS_FTP_INI_Attack

This exploit gets the ws_ftp.ini file from a windows host.

Applicable Operating Systems:

- Network- or Application-based attack

X_Server_Crash_Attack

This exploit attemps to remove a file from the X-Server which can crash the system.

Applicable Operating Systems:

- Windows NT
- Windows 95 / 98
- UNIX
- Solaris
- Sun OS
- HP / UX
- AIX
- Linux

Index

A

About NetProwler
  Help menu option 3.7
Absolute URL from Web Server Root Directory box 8.4
access
  deleting an entry 8.24
  modifying an entry 8.22
  restricting network (overview) 1.8
  restricting to the network 8.20
Access branch (tour) 3.21
  restricting network access (tour) 3.33
access restrictions
  adding new (via the toolbar) 3.8
ACK flag. See TCP_ACK.
actions
  configuring for an attack signature 5.12, 6.16, 6.19
  in response to an attack (overview) 1.3
  methods of configuring 6.21
  notification defined 6.19
  overview 1.9
  responses defined 6.19
Actions box 6.16
  in the ASD Wizard 7.38
Add License dialog box 2.10, 4.2
Add New button 5.16, 5.18
Add New button (toolbar) 3.8
Add Search Primitive button
  described 7.16
Add Value Primitive button 7.19
adding
  applications to the Application Book .. 4.22
  systems to the Address Book manually 5.16
  systems using the Profiler 5.3
  user-defined attack signatures 7.32
Address Book
  adding
    a range of systems 5.18
    a single system 5.16
    systems using the Profiler 5.2
    systems via the Profiler (tour) 3.16
  building (overview) 5.1
  configuring Applications (overview) .. 4.21
  deleting entries from 5.19
  overview 3.23
Address Book Entry dialog box 5.17
Address Entry Name edit box 5.17, 5.18
address mask reply
  ICMP message type 7.23
address mask request
  ICMP message type 7.23
adjusting
  an attack signature's priority 6.16, 6.18
administering NetProwler 4.1
Administration menu (tour) 3.6
Alarm Threshold box 3.30
Alarm Type list box 10.16

Alarm Types box 10.9
Alerts
resetting 3.8
alerts
resetting 9.3
viewing 9.2
Alerts branch (tour) 3.30
Alerts database 9.3
querying 10.15
Allowed Time box 8.21
alternate host address
ICMP message type 7.23
analyze data
step 2 in development process 7.4
AND operator 7.26
Apache_Web_Server_D_O_S_Attack ... C.2
application
adding to the Application Book 4.22
deleting from Application Book 4.24
modifying an attack signature's 6.15
modifying in the Application Book 4.24
setting up an 4.21
Application Book
adding an application 4.22
deleting an application 4.24
modifying an application 4.24
Application Entry field 4.22
Application list box 10.16
Application Type box 4.22
application types
FTP-like 4.23
Generic 4.23
HTTP / UDP-like 4.23
Applications Book
adding entries (via the toolbar) 3.8
overview 3.24
Applications box 6.15, 7.13
Edit Attack Association Details dialog box 5.12
in the ASD Wizard 7.37
Applied Attacks box 5.8
associating 6.14
disassociating 6.17
Applies To box 7.13, 7.34
in the ASD Wizard 7.37
applying
attack signatures 5.8
ARP_Host_Down_Check C.2
ASCEND_ROUTE_ASCEND_KILL C.3
ASCII radio button
described 7.16
ASD Wizard
Tools menu option 3.7
Associate Priorities branch (tour) 3.27
associating
attack signatures manually 6.13
methods of 6.13
Attack Association branch (tour) 3.13
Attack branch (tour) 3.10, 3.31
Attack Details report
overview 1.10
scheduling 10.8
Attack Details report (tour) 3.22
attack signature
changing the priority level 6.16, 6.18
configuring actions 6.16, 6.19
configuring actions by 6.24
deleting 6.18
disassociating 6.16
Attack Signature Definition toolkit .. 7.1, 7.4
Attack Signature Definition Wizard
using 7.35
Attack Signature Definition (ASD) toolkit
touring 3.12
understanding 7.5
Attack Signature Detection
understanding 1.4
Attack Signature Type box 7.33

attack signatures 5.12
actions (overview) 1.9
adding (via the toolbar) 3.8
applying to profiled systems 5.8
associating manually 6.13
categories 7.3
changing the priority level 5.12
Common
adjusting
Denial of Service threshold 6.9
Ping of Death settings 6.12
Port Scan threshold 6.8
SYN Flood threshold 6.9
TCP/IP Spoofing settings 6.10
Denial of Service 6.4
Man in the Middle 6.6
modifying 6.8
overview 3.10, 6.2
Ping of Death 6.5
Port Scan 6.3
SYN Flood 6.3
TCP/IP Spoofing 6.4
configuring
an authorized source 6.15
creating 7.32
building expressions 7.28
collecting data 7.3
prerequisite knowledge 7.2
using the ASD Wizard 7.35
(overview) 7.1
Custom
defined 6.7
described 3.10
listed C.2
defined 6.1
development process 7.2
analyze data 7.4
create signature 7.4
generate and collect data 7.3
test and debug 7.5
disassociating 6.16
importing 4.5
methods of associating 6.13
modifying (from within the Profiler) 5.11
prerequisite knowledge 7.39
properties
delimiter-based 7.13
Distinguish Attackers 7.12
overview 7.12
selecting applicable applications ... 7.13
selecting applicable operating systems 7.13
tutorials
counter-based 7.49
data-specific 7.40
network-specific 7.45
overview 7.39
types 6.2
Counter-based 7.10, 7.33
overview 7.9
Sequential-based 7.11, 7.33
Simple 7.9, 7.33
user-defined 3.10, 6.8
Attack Template Name box
in the ASD Wizard 7.37
attacks
configuring authorized sources of. 6.15
monitoring detected 9.2
viewing all detected 9.2
viewing by attack type 9.4
Authentication Enabled check box 4.16, 8.17
Authentication String field 8.17
Authorized box 6.15
Edit Attack Association Details dialog box 5.12
authorized sources of an attack 5.12
specifying 6.15
Automatic radio button 2.11

Available Attacks box..... 6.14
Average cost of unavailability per server field 10.6
AXENT
licensing phone number A.10
AXENT Online web services
about A.4
AXENT Services
about A.11

B

BackOrifice_Detect..... C.3
Bonk_Attack..... C.3
Brute_Force_Login_Attempt..... C.4
Byte..... 7.18
Byte radio button
Value Primitives tab 7.18

C

capture session action
configuring by attack signature..... 6.24
defined..... 6.21
overview..... 1.9
Capture Session To File dialog box 9.10
captured sessions
deleting..... 4.27
replaying (via the toolbar)..... 3.8
used to create attack signatures..... 7.3
viewing..... 3.32, 9.5
capturing
live sessions 9.9
live sessions (overview)..... 1.7
Cascade
Windows menu option 3.7
Case Sensitive Search check box
described 7.16
Change button
used to schedule the Profiler 5.14
Change Password
Administration menu option.....3.6
changing
the administrative password 4.3
Client IP Address field.....10.16
comma-separated (CSV) report
viewing 10.14
Common attack signatures.....6.2
Common attacks
configured in the Profiler 5.3
described.....3.10
Common Attacks to be Configured box
on the Profiler Schedule dialog box5.14
on the Start Scan dialog box.....5.5
Communication Devices branch (tour) 3.26
Configure
Windows menu option 3.7
Configure button 5.7
Configure tree and pane.....3.9
Configure window (overview).....3.5
configuring
actions 5.12, 6.21
by attack signature.....6.24
by priority level 6.22
by priority level (tour).....3.27
actions (tour) 3.27
an authorized source of attack 5.12
e-mail action capabilities 3.27
firewall hardening capabilities.....3.25
pager action capabilities.....3.26
SNMP capabilities 3.25
systems via the Profiler 3.16, 5.2
connection-based attacks.....7.3
Consistency branch
Configure window (tour).....3.33
Monitor window (tour) 3.18

consistency checking
configuring Web server 8.2
deleting a DNS consistency check entry 8.15
deleting a router entry 8.19
deleting a Web server entry 8.6
deleting an FTP server entry..... 8.11
modifying a DNS table entry..... 8.14
modifying a FTP server entry 8.9
modifying a routing table entry 8.18
modifying a Web server entry 8.5
overview 1.7
securing a DNS table..... 8.12
securing a routing table 8.16
securing a Web server..... 8.2
securing an FTP server..... 8.7
consulting services..... A.11
contacting
technical support. See customer support.
Contents
Help menu option..... 3.7
contents
of this manual..... 1.12
conversations
capturing live 9.9
configuring monitoring 9.5
monitoring (overview)..... 1.6, 9.1
terminating live..... 9.8
viewing captured..... 9.11
viewing live 9.7
viewing saved 9.11
Conversations Branch (tour) 3.20
Conversations branch (tour) 3.32
Cookie_Monster_Attack_Decode.....C.4
Cost Analysis report..... 10.5
overview 1.11
scheduling..... 10.5
Cost Analysis report (tour)..... 3.22
Counter-based
attack signature type.....7.10
CPU
upgrading to improve performanceB.3
utilization at 100 percent..... B.3
create attack signature
step 2 in development process 7.4
creating
a LAND attack signature 7.46
an attack signature 7.32
attack signatures (overview) 7.1
complex expressions.....7.29
custom attack signatures (overview)1.5
expressions (overview).....7.28
simple expressions 7.28, 7.29
Custom attack signatures.....6.7
described 3.10
listed C.2
Custom Attacks branch 3.11
Custom radio button.....2.12
Customer Satisfaction Assistant
about.....A.4
customer support
about.....A.7
steps before contacting A.7

D

data analysis
step 2 in development process 7.4
data collection
step 1 in development process 7.3
debug
step 4 in development process 7.5
Default Operating System edit box 5.15
Delete button
in the Address Book.....5.19

deleting
a DNS consistency check entry 8.15
a limit access entry 8.24
a report 10.14
a router consistency check entry 8.19
a scheduled report 10.12
a Web server consistency check 8.6
Address Book entries 5.19
an attack signature 6.18
an FTP consistency check 8.11
captured sessions 4.27
delimiter-based
check box 7.34
described 7.13
De-militarized Zone (DMZ)
deploying NetProwler in 2.5
Denial of Service
Common attack signature
adjusting the threshold settings 6.9
description of 6.4
deploying
NetProwler
behind a firewall 2.6
in a De-militarized Zone (DMZ) 2.5
in a server farm 2.6
on a switched network 2.6
overview 2.3
Description field
attack signature definition 7.8
Attack Signature Definition dialog 7.33
Search Primitive tab 7.15
Value Primitives tab 7.17
destination address (in the IP header). See IP_DEST_ADDRESS.
destination port (in the TCP header). See TCP_DEST_PORT.
destination port (in UDP header). See UDP_DEST_PORT.
destination unreachable
ICMP message type 7.23
Details button
Edit Attack Association dialog box .. 5.9
DIG-Attack C.5
Disable Configuration button 5.10
disabling
a report without deleting it 10.12
disassociating
an attack signature 6.16
Distinguish Attackers
described 7.12
Distinguish Attackers check box 7.33
DNS Consistency Check dialog box 8.12
DNS Server Name field 8.13
DNS server resources
deleting a consistency check entry. 8.15
DNS table
modifying a consistency check entry 8.14
securing 8.12
securing (overview) 1.7
securing (tour) 3.19, 3.33
DNS_REQUEST_BROADCAST C.5
DNS_Zone_Transfer_Decode C.6
Double Word radio button 7.18
Duplicate-IP-Address-Detection C.6
Duration box 10.16
dynamic attack signature definition
understanding 1.5
Dynamic check box 7.18
Dynamic Host Configuration Protocol (DHCP) environments
not using the Profiler in ... 5.3, 5.13, 5.16

E

echo reply
ICMP message type 7.23

echo request
ICMP message type 7.23
Echo_Chargen_loop_Attack C.7
Edit Attack Association Details dialog box 5.12
tour 3.15
Edit Attack Association dialog box
overview 3.14
using 5.8, 5.11
Edit DNS Consistency Checking dialog box 8.14
Edit FTP Server Consistency Check dialog box 8.10
Edit Host Entry dialog box 8.23
Edit Router Consistency Checking 8.18
Edit Web Server Consistency Check dialog box 8.5
e-mail
a scheduled report. 10.4
action
configuring by attack signature 6.24
introducing 3.25
overview 1.9
setting up the capability for 4.9
E-mail Address edit box 4.10
E-mail To action
scheduled reports 10.4, 10.7, 10.10
E-mail_From_Decode C.7
E-mail_To_Decode C.8
Ending Address box 5.18
Enter IP Address or Range box
Start Scan dialog box 5.4
escalation procedures A.4
Execute Command action
scheduled reports 10.4, 10.7, 10.10
Executive Summary report
overview 1.11
scheduling 10.2
Executive Summary report (tour) 3.22
Exit
File menu option 3.6
Exit this install option
retain existing installation 2.15
exiting
NetProwler 3.37
Expected Tolerances
defined 10.3
entering percentage values 10.3
Export To action
scheduled reports 10.4, 10.7, 10.10
expressions
building 7.28
creating complex 7.29
creating simple 7.28, 7.29
operators
arithmetic 7.27
bit-wise 7.26
combination 7.27
equality 7.27
logical 7.26
overview 7.26
types
complex 7.28
reserved keywords 7.28
simple 7.28
single primitives 7.28
using single primitives or keywords 7.28
Expressions tab 7.7
overview 7.14
Reserved Keywords tab 7.19
Search Primitives tab 7.14
Value Primitives tab
understanding 7.17
External option
TCP / IP Spoofing type 6.11
Extract at offset __ from the start of __ Payload option
Value Primitives tab 7.19

F

failed logins attack signature
tutorial overview 7.49
File menu (tour) 3.6
FIN flag (in the TCP header). See TCP_FIN.
Finger_User_Decode C.8
firewall
deploying NetProwler behind 2.6
firewall hardening action
configuring by attack signature 6.24
defined 6.20
overview 1.9
firewall notification action
setting up Firewall-1 ..... 4.14
setting up Raptor Firewall 4.11
Firewall-1 firewall hardening
introducing 3.25
Force Capitals check box 7.18
fragment flag. See IP_FRAGMENTS and IP_MORE_FRAGMENTS
fragment offset. See IP_FRAGMENT_OFFSET.
Frame Statistics box B.2
Frames Dropped field 3.28, B.2
Frames Processed field 3.28, B.2
Frequency
Schedule Report Entry dialog box 10.4, 10.7, 10.9
Frequency box 10.6
FTP
attack signature tutorial 7.40
viewing live sessions 9.7
FTP Consistency Check dialog box 8.8
FTP server files
securing (overview) 1.8
securing (tour) 3.19, 3.33
FTP Server Name field 8.8
FTP Server Password field 8.9
FTP Server Port field 8.8
FTP server resources
deleting a consistency check entry 8.11
modifying the configuration 8.9
securing 8.7
FTP Server User field 8.8
FTP-CWD-Vulnerability C.8
FTP-MKDIR-Decode C.9
FTP-PUT-Decode C.10
FTP-RMDIR-Decode C.11
FTP-Root-User-Access-Decode C.11
FTP-Scan C.12
FTP-SITE-EXEC-Vulnerability C.12
FTP-SITE-Vulnerability C.13
FTP-USER-Decode C.13
FTP_Arg_Core_Dump_Decode C.14
FTP_Get_File_Decode C.9
FTP_Password attack signature tutorial
creating 7.41
triggering 7.44
viewing 7.45
FTP_Password_Decode C.10

G

General tab
described 7.6
using 7.8
generate and collect data
step 1 in development process 7.3
Generated Reports branch (tour) 3.35
generating
reports 10.15
overview 1.10
tour 3.35
user-defined (tour) 3.36
reports (overview) 10.1
Global Online Incident
about A.4

H

harden firewall action
configuring by attack signature..... 6.24
defined..... 6.20
introducing 3.25
overview 1.9
Help
accessing via the toolbar..... 3.8
sources of A.1
using 4.28
Help menu (tour) 3.7
Hex radio button..... 7.16
High priority (defined) 6.22
Host Address edit box..... 5.17
Host Details dialog box..... 5.7, 5.11
Host radio button..... 5.17
Host Response Timeout box
Profiler Schedule dialog box..... 5.15
Start Scan dialog box..... 5.5
HPUX-RemoteWatch-Vulnerability.....C.15
HP_UX_NETTUNE_Attack C.14
HP_UX_PPL_EXPLOIT_Attack.....C.15
HTML files
securing..... 8.2
securing (tour)..... 3.19, 3.33
HTML reports
viewing..... 10.13
HTTP-Campas-CGI-Vulnerability C.16
HTTP-Convert-CGI-BIN-VulnerabilityC.16
HTTP-Glimpse-Vulnerability.....C.17
HTTP-Java-Decode C.17
HTTP-NPH-TEST-Vulnerability.....C.18
HTTP-PHF-CGI-Vulnerability.....C.18
HTTP-SGI-Wrap-Vulnerability.....C.19
HTTP-TEST-Vulnerability C.19
HTTP-View-Source-Script-VulnerabilityC.20
HTTP_BAT_FILE_EXEC.....C.20
HTTP_COUNT_CGI_DECODE C.20
HTTP_ETC_PASSWD_DECODE..... C.21
HTTP_EXEC_ISP_FILE C.21
HTTP_UPLOADER_DECODE..... C.22
HTTP_WIN_C_SAMPLE_DECODE_ASD. C.22

I

ICMP
header parameters.....7.23
nonconnection-based attacks.....7.3
reserved keyword 7.20
ICMP Datagrams field 3.29
Others field..... B.2
ICMP Echo Request. See Denial of Service
ICMP message types 7.23
ICMP_Dst_Proto_Unreachable_DecodeC.23
ICMP_Redirect_Host_Redirect_Message ... C.23
ICMP_Redirect_Net_Redirect_MessageC.24
ICMP_Redirect_Packet C.24
ICMP_Redirect_TOS_Host_Redirect_Message C.25
ICMP_Redirect_TOS_Net_Redirect_Message C.25
ICMP_SMURF..... C.26
ICMP_TYPE
reserved keywords.....7.23
IDENT-Newline-Vulnerability..... C.26
IDENT-User-Decode..... C.27
IMAP_Username_Password_Decode . C.27
importing
attack signatures.....4.5
incident reporting procedures.....A.4
information reply
ICMP message type 7.23
information request
ICMP message type 7.23

Information Security SWAT Web Site
about A.5
installing
NetProwler..... 2.8
overview 2.1
requirements..... 2.2
integrating with Intruder Alert..... 1.9, 4.19
Intelligent radio button
Profiler Schedule dialog box 5.15
Start Scan dialog box 5.5
Internal
TCP/IP Spoofing type..... 6.11
INVALID_TCP_FRAME_DETECT C.28
INVALID_TTL_DECODE..... C.28
IP
header parameters 7.21
reserved keyword 7.20
IP Address column
DNS Consistency Check dialog box8.13
IP Address Spoofing check box 6.12
IP datagram length. See IP_TOTAL_LENGTH.
IP header length. See IP_HLEN.
IP identification number. See IP_IDENTIFICATION.
IP spoofing. See TCP/IP Spoofing.
IPVERS
reserved keyword 7.21
IP_DEST_ ADDRESS
reserved keyword 7.22
IP_FRAGMENT
reserved keyword 7.21
IP_FRAGMENT_OFFSET
reserved keyword 7.21
IP_HLEN
reserved keyword 7.21
IP_IDENTIFICATION
reserved keyword 7.21
IP_MORE_ FRAGMENTS
reserved keyword.....7.21
IP_Options_Loose_Source_Routing_Decode C.29
IP_Options_Record_Route_Decode.....C.29
IP_Options_Security_Enabled_DecodeC.30
IP_Options_Strict_Source_Routing_Decode C.30
IP_Options_TimeStamp_Decode C.31
IP_PROTOCOL
reserved keyword.....7.22
IP_SRC_ ADDRESS
reserved keyword.....7.22
IP_TOTAL_ LENGTH
reserved keyword.....7.21
IP_TTL
reserved keyword.....7.21
IP_Unknown_Protocol.....C.31
IRC
viewing live sessions.....9.7
IRC_Channel_Decode.....C.32
IRC_Message_Decode.....C.32
IRC_Nick_Decode C.32

L

LAND attack C.33
attack signature tutorial 7.45
LATIERRA.....C.33
license
updating.....4.2
License Key field
Add Licenses dialog box 2.10, 4.2
License Key Requests
about..... A.4
license requirements 2.3
licensing
phone number..... A.10
procedures..... A.4

links
to other security resources A.12
LINUX-Dump-Command-VulnerabilityC.33
LINUX-KBD-Denial-of-service C.34
LINUX-Login-Command-VulnerabilityC.34
LINUX-Login-Vulnerability.....C.35
LINUX_LOGIC_BOMB_Attack.....C.35
LINUX_SHADOW_FILE_Attack C.36
Low priority (defined)..... 6.22

M

MAC Header
in Search Primitive 7.15
in Value Primitive..... 7.19
Mail Server IP Address edit box,..... 4.10
Man in the Middle
attack signature..... 6.6
manual
about..... A.3
contents 1.12
Maximum ICMP Datagram Size field . 6.13
Maximum TCP Segment Size field..... 6.13
Maximum UDP Segment Size field..... 6.13
Medium priority (defined) 6.22
memory
increasing to improve performance B.3
Menu Bar..... 3.6
MICRO_FRAGMENT_DETECT.....C.36
Mirror Server Name field 8.8
Mirror Server Name list box 8.3
Mirror Server Password field
FTP..... 8.9
Web server..... 8.3
Mirror Server Port field
FTP..... 8.8
Mirror Server Start Directory box 8.9
Mirror Server Start Directory field..... 8.4
Mirror Server User field
FTP.....8.8
Web server.....8.3
modifying
a DNS table entry 8.14
a FTP server consistency check entry8.9
a limit access entry 8.22
a report's generation schedule 10.11
a routing table's consistency check entry 8.18
Web server consistency check entries8.5
Monitor
Windows menu option.....3.7
Monitor tree and pane 3.28
Monitor window (overview) 3.5
monitoring
attacks 9.2
live network sessions.....1.6, 9.1
network conversations 9.5
starting and stopping NetProwler...3.8
MS-IE-LNK-Vulnerability..... C.37
MS-IE-URL-Vulnerability C.37
MS-WIN-Remote-Passwd-Access..... C.37
MS-WIN-Remote-Registry-Access..... C.38
MS_IIS_ASP_Attack..... C.38
MS_JOLT_Attack..... C.38
MS_WIN_SAM_ACCESS..... C.39

N

Name field
attack signature definition 7.8
Search Primitive tab.....7.15
Value Primitives tab.....7.17
NetProwler
administering (overview).....4.1
Console
Changing the password 4.3

Console (tour) 3.4
deploying
behind a firewall 2.6
in a server farm 2.6
on a switched network 2.6
overview 2.3
description 3.1
features (overview) 1.3
installing 2.8
overview 2.1
requirements 2.2
integrating with Intruder Alert 1.9
introducing 1.1
performance
improving B.3
monitoring B.2
optimizing (overview) B.1
reports
deleting 10.14
deleting scheduled 10.12
generating user-defined 10.13
modifying scheduled 10.11
overview (tour) 3.22
scheduling 10.2
turning off scheduled 10.12
types of 10.1
viewing 10.13
starting 3.2
stopping 3.37
Toolbar 3.8
touring 3.1
training A.5
uninstalling 2.11
upgrading 2.13
NetProwler Authentication dialog box 3.3, 4.3
NetProwler database
purging 4.25
NetProwler Install Found dialog box ... 2.15
NetProwler License dialog box 2.9, 2.14
Netprowler.mdb 4.25
NetRecon
used to scan ports 6.3
Netscape_Cache_Cow_Attack_Decode C.39
Netscape_Son_Of_Cache_Cow C.39
network
deploying NetProwler
behind an Internet firewall 2.6
in a DMZ 2.5
in a server farm 2.6
on a switched network 2.6
profiling 5.2
(overview) 1.5
restricting access to 8.20
restricting access (overview) 1.8
sessions
monitoring 1.6, 9.5
Network Devices branch 3.25
network frame
payload options in Search Primitives ... 7.15
payload options in Value Primitives 7.19
network interface card (NIC)
placed in promiscuous mode 1.2
network requirements
for installing NetProwler 2.3
New Time of Day Access Entry dialog box 8.21
NewTear C.40
NFS-EXPORT-Command-Decode C.40
NNTP_Group_Decode C.40
NNTP_Password_Decode C.41
NNTP_Username_Decode C.41
nonconnection-based attacks
ICMP 7.3
UDP 7.3
NOT operator 7.26

notification actions
configuring in response to an attack6.19
defined..... 6.19
introduction to 1.9
methods of configuring 6.21
setting up e-mail 4.9
setting up Firewall-1 ..... 4.14
setting up overview..... 4.7
setting up pager 4.8
setting up Raptor Firewall..... 4.11
setting up SNMP..... 4.19
Notification List Services..... A.4
Notification Options branch..... 3.25
NT-DNS-QR-Bit-Vulnerability C.41
NT-IIS-Telnet-GET-Vulnerability.....C.42
NT-PortMapper-Flood C.42
NT-Telnet-denial-of-service C.42
NT_DNS_Attack C.42

O

Online Help
about..... A.2
OOB_Attack_ON_NT.....C.43
Open Database Connectivity (ODBC) services
stop all before installing 2.9
Open Platform for Secure Enterprise Computing (OPSEC)..... 4.14
opening
a saved conversation..... 9.11
Operating System drop-down list box
Address Book Entry dialog box..... 5.17
Operating Systems box 7.13
ASD Wizard..... 7.37
operators
arithmetic..... 7.27
bit-wise..... 7.26
combination 7.27
equality 7.27
logical.....7.26
overview 7.26
Options
Tools menu option 3.7
OR operator.....7.26
Others field.....3.29

P

pager action
configuring by attack signature 6.24
configuring by priority level 6.23
defined 6.20
introducing.....3.25
overview 1.9
setting up capabilities for.....4.8
parameter problem
ICMP message type 7.23
password
changing 4.3
required length 4.4
payload
MAC.....7.15, 7.19
Network.....7.15, 7.19
Raw.....7.15, 7.19
Transport.....7.15, 7.19
Perform Uninstall box.....2.12
performance
improving..... B.3
monitoring..... B.2
optimizing (overview)..... B.1
perimeter network
deploying NetProwler in 2.5
See De-militarized Zone (DMZ)
ping flood denial of service attack.....6.4

Ping of Death attack
adjusting threshold settings 6.12
described 6.5, 7.3
PING_REPLY_FLOOD..... C.43
policies
product support A.4
POP3
viewing live sessions 9.7
POP_Password_Decode..... C.44
POP_Username_Decode C.44
Port Response Timeout box
Start Scan dialog box 5.5
Port Scan attack signature
adjusting the threshold settings..... 6.8
described 6.3
ports
primary application 4.23
secondary application 4.23
Ports and Applications box
on the Host Details dialog box..... 5.7
predefined attack signatures. See Custom attack signatures.
Priority drop-down list box..... 6.16
priority level 3.27
changing..... 5.12, 6.16, 6.18
configuring actions by..... 6.22
default setting..... 6.22
high (defined)..... 6.22
low (defined) 6.22
medium (defined)..... 6.22
Priority Level list box 5.12
Priority list box 10.16
product support policy A.4
Product Upgrade Requests..... A.4
Profile Now
Tools menu option..... 3.7
Profile Now button 3.8
about 3.16
starting the Profiler..... 5.4
profiled system
configuring with attack signatures ..5.6
removing.....5.9
Profiler
configuring a profiled system.....5.6
introducing.....1.5
removing a profiled system 5.9
scheduling 5.13
scheduling (tour) 3.18
starting 5.3
touring the 3.16
using 5.2
Profiler Schedule dialog box.....5.14
promiscuous mode
network interface card.....1.2
Properties box 7.33
Protocol box.....4.23
Router Consistency Check dialog box.. 8.17
Protocol Distribution box B.2
protocol field (in the IP header). See IP_PROTOCOL.
protocol types
reserved keywords.....7.20
PSH flag. See TCP_PSH.
Purge button (toolbar) 3.8
Purge Database
Administration menu option.....3.6
purging
Alerts database 3.8, 4.25

Q

query
saving a user-defined.....10.17
the Alerts database.....3.36, 10.15
Query Parameters branch (tour) 3.36

R

Range radio button
Address Book Entry dialog box..... 5.18
ranges
adding to the Address Book manually 5.18
Raw
payload type..... 7.15, 7.19
redirect
ICMP message type..... 7.23
Release Notes
about..... A.3
Remote_Packet_Capture_Decode C.45
removing
a scheduled report..... 10.12
attack signatures..... 6.18
captured sessions..... 4.27
DNS consistency check entries 8.15
entries from the Address Book..... 5.19
FTP consistency check entries..... 8.11
limit access entries..... 8.24
reports 10.14
router consistency check entries.... 8.19
Web server consistency check entries8.6
Replay button (toolbar)..... 3.8
Replay Session
File menu option..... 3.6
Report Name field 10.3
Schedule Reports Entry dialog box10.9
Report Type list box 10.3, 10.6, 10.9
report types
overview 10.1
reports
Attack Details..... 1.10
Cost Analysis..... 1.11, 10.5
deleting..... 10.14
deleting scheduled..... 10.12
disabling w/o deleting 10.12
Executive Summary.....1.11, 10.2
generating.....3.8, 10.2
overview.....1.10, 10.1
user-defined.....3.36, 10.15
modifying scheduled.....10.11
saving.....10.17
scheduling.....10.2
temporarily disabling.....10.12
types.....3.22
viewing.....10.13
viewing generated (tour) 3.35
Reports branch (tour).....3.22, 3.35
requirements
for installing NetProwler 2.2
rescanning
with the Profiler.....3.18
reserved keywords
building an expression with only one.. 7.28
ICMP 7.20
ICMP header parameters 7.23
ICMP_TYPE 7.23
IP.....7.20
IP header parameters.....7.21
IPVERS.....7.21
IP_ PROTOCOL.....7.22
IP_DEST_ADDRESS 7.22
IP_FRAGMENT.....7.21
IP_FRAGMENT_OFFSET 7.21
IP_HLEN 7.21
IP_IDENTIFICATION 7.21
IP_MORE_FRAGMENTS.....7.21
IP_SRC_ADDRESS.....7.22
IP_TOTAL_LENGTH 7.21
IP_TTL.....7.21
protocols 7.20
TCP.....7.20
TCP_ACK.....7.24
TCP_DEST_PORT 7.24

TCP_FIN 7.25
TCP_HLEN 7.24
TCP_PSH 7.24
TCP_RST 7.25
TCP_SRC_PORT 7.24
TCP_SYN 7.25
TCP_SYNACK 7.25
TCP_URG 7.24
TCP_WINDOWSIZE 7.25
True 7.19
types of 7.19
UDP 7.20
UDP_DEST_PORT 7.24
UDP_MSG_LEN 7.24
UDP_SRC_PORT 7.24
understanding 7.19
used in complex expressions 7.29
used in simple expressions 7.28
Reset Alerts button (toolbar) 3.8
Reset button 7.19
described 7.16
reset flag (in the TCP header). See TCP_RST.
reset session action
configuring by attack signature 6.24
defined 6.20
overview 1.9
resetting
Alerts 3.8
alerts 9.3
Resolve Now button 5.17
resolving an IP address 5.17
response actions
defined 6.19
methods of configuring 6.21
overview 1.9
restricting
access to the network 8.20
access to the network (overview) 1.8
access to the network (tour) 3.21
RFC 1700 ..... 4.21
RIP radio button 8.17
RIP2 radio button 8.17
rLogin
delimiter-based application 7.13
viewing live sessions 9.7
RLogin_Vulnerability_Attack C.45
router
deleting a consistency check entry 8.19
TCP/IP Spoofing type 6.11
router advertisement
ICMP message type 7.23
router configuration tables
securing 8.16
Router Consistency Check dialog box ..8.17
Router Name list box 8.17
router solicitation
ICMP message type 7.23
router tables
modifying a consistency check entry 8.18
securing (overview) 1.8
securing (tour) 3.19, 3.33
rSH
delimiter-based application 7.13
viewing live sessions 9.7
RST flag (in the TCP header). See TCP_RST.

S

saving
a user-defined report 10.17
scanning
ports 6.3
the network for systems 3.16
Schedule Reports Entry dialog box 10.3, 10.6, 10.9
Scheduled check box 10.12

scheduling
Attack Details report 10.8
Cost Analysis report..... 10.5
Executive Summary report 10.2
reports 10.2
the Profiler 3.18, 5.13
SDSI. See Stateful Dynamic Signature Inspection.
Search at offset __ from the start of __ payload radio button 7.15
Search Entire __ Payload radio button 7.15
Search Primitive Name field
ASD Wizard..... 7.36
Search Primitive Pattern field
ASD Wizard..... 7.36
search primitives
building an expression with only one . 7.28
understanding..... 7.14
used in complex expressions 7.29
used in simple expressions..... 7.28
securing
DNS tables 1.7, 8.12
FTP server resources 8.7
FTP server (overview)..... 1.8
network resources (overview) .. 1.7, 8.1
network resources (tour) 3.18
router configuration tables..... 8.16
router configuration tables (overview) 1.8
Web server files..... 8.2
Web server files (overview) 1.8
Security Forum
about..... A.5
security resources
links A.12
Select Destination Directory dialog box2.10
Select Directories to Remove box 2.12
Select Private Files to Remove box,..... 2.12
Select Registry Keys to Edit box.....2.12
Select Registry Keys to Remove box.....2.12
Select Sub-systems to Remove box 2.12
Select System Files to Remove box 2.12
Selected Attacks box 6.14, 6.19, 6.24
Edit Attack Association dialog box .5.9
send e-mail action
defined 6.20
Send Suspicious Messages check box...4.16
Sequential-based
attack signature type.....7.11
server farm
deploying NetProwler in 2.6
Server list box
New Time of Day Access Entry dialog box 8.21
Server Name list box.....10.16
Service list box
New Time of Day Access Entry dialog box 8.21
session
monitoring.....9.5
sessions
capturing action (overview) 1.9
capturing live.....9.9
capturing (overview) 1.7
monitoring (overview) 1.6
replaying captured.....3.8
reset action (overview) 1.9
terminating live 9.8
terminating live (overview).....1.7
viewing captured 9.5, 9.11
viewing live.....9.7
viewing live (tour).....3.32
viewing saved 9.11
setting
attack signature priority levels6.16, 6.18

setting up
applications 4.21
e-mail notification capabilities 4.9
Firewall-1 notification capabilities 4.14
notification capabilities 4.7
pager notification capabilities 4.8
Raptor Firewall notification capabilities 4.11
SNMP notification capabilities 4.19
Show Routes button 8.17
Signed Value check box
described 7.18
Simple
attack signature type 7.9, 7.33
simple expressions
creating 7.28, 7.29
SMTP
viewing live sessions 9.7
SMTP mail server
setting up e-mail notification capabilities 4.10
SMTP-DEBUG-Decode C.46
SMTP-EXPN-Decode C.46
SMTP-Piped-Command-Vulnerability C.47
SMTP-QMAIL-Vulnerability C.47
SMTP-VRFY-Decode C.48
SMTP-WIZ-Decode C.48
Smurf attack signature C.26
SNMP notification
setting up 4.19
SNMP trap action
configuring by attack signature 6.24
configuring by priority level 6.23
defined 6.20
introducing 3.25
overview 1.9
source address (in the IP header). See IP_SRC_ADDRESS.
source port (in the TCP header). See TCP_SRC_PORT.
source port (in the UDP header). See UDP_SRC_PORT.
source quench
ICMP message type 7.23
spawn a command action
configuring by attack signature 6.24
defined 6.21
overview 1.9
Start Address box 5.18
Start Monitoring button 3.8
Start Scan dialog box 1.5, 3.16, 5.4
starting
NetProwler 3.2
network monitoring 3.8
Stateful Dynamic Signature Inspection (SDSI)
described 1.4
Statistics branch (tour) 3.28
Stop Monitoring
File menu option 3.6
Stop Monitoring button 3.8
stopping
NetProwler 3.37
network monitoring 3.8
String __ Characters Long Radio button 7.18
SunOS-UDP-Bomb C.49
SunOS_AUDIOOCTL_KERNEL_PANIC ... C.49
SunOS_dev_nit_exploit C.50
SunOS_DF_Attack C.50
SunOS_Keyboard_Kernal_Panic C.51
SunOS_Not_On_System_Console C.51
SunOS_Ping_Crash_Attack C.51
SunOS_TCP_Kernal_Panic C.52
SunOS_TCX0_Kernal_Panic C.52

Suspicious Activity Monitoring Protocol (SAMP)
introducing 3.25
used to harden firewall..... 4.14
SYN flag (in the TCP header). See TCP_SYN.
SYN Flood
Common attack signature
adjusting threshold settings..... 6.9
described..... 6.3
SYN Flood threshold
settings 6.4
SYNACK. See TCP_SYNACK.
Sync New Signatures
Administration menu option 3.6
See importing attack signatures
SynDrop C.53
Syslog_fogger C.53
system requirements 2.2
systems
adding manually..... 5.16
adding new (via the Profiler).... 3.8, 5.2
profiling and configuring (overview).. 3.16

T

tab-separated (TSV) report
viewing..... 10.14
TCP
connection-based attacks..... 7.3
reserved keyword..... 7.20
three-way handshake..... 6.3
TCP header parameters 7.24
TCP Segments field.....3.29, B.2
TCP Sequence No. Spoofing check box6.12
TCP/IP
LAND attack 7.45
restricting access
configuring.....8.20
on applications (tour) 3.33
overview.....1.8
TCP/IP Illustrated Volume 1
The Protocols 7.2
TCP/IP Spoofing
Common attack signature
adjusting the settings.....6.10
described 6.4
eliminating false positive alarms6.10
types of
External.....6.11
Internal 6.11
Router 6.11
TCP/IP version. See IPVERS
TCP_ACK
reserved keyword 7.24
TCP_DEST_ PORT
reserved keyword 7.24
TCP_FIN
reserved keyword 7.25
TCP_HLEN
reserved keyword 7.24
TCP_PSH
reserved keyword 7.24
TCP_RST
reserved keyword 7.25
TCP_SRC_PORT
reserved keyword 7.24
TCP_SYN
reserved keyword 7.25
TCP_SYNACK
reserved keyword 7.25
TCP_URG
reserved keyword 7.24
TCP_WINDOWSIZE
reserved keyword 7.25
TearDrop.....C.54

Technical Support Policies and Procedures
about A.4
telnet
delimiter-based application..... 7.13
viewing live sessions 9.7
Telnet-detect C.54
Telnet-Potential-Denial-of-Service C.54
Telnet_3Failed_Logins attack signature
creating 7.49
triggering..... 7.53
viewing 7.54
terminating
live sessions 1.7, 9.8
See reset session action.
test
step 4 in development process..... 7.5
TFTP_GET_Vulnerability C.55
TFTP_PUT_Vulnerability_Attack..... C.55
three-way handshake 6.3
threshold settings
adjusting
Denial of Service 6.9
Ping of Death..... 6.12
Port Scan 6.8
SYN Flood..... 6.9
TCP/IP Spoofing 6.10
Tile
Windows menu option 3.7
time exceeded
ICMP message type 7.23
Time of Day Access..... 3.33, 8.20
time to live (TTL) field (in the IP header). See IP_TTL.
timestamp reply
ICMP message type 7.23
timestamp request
ICMP message type 7.23
toolbar..... 3.8
Tools menu..... 3.7
tour
NetProwler 3.1
starting 3.2
tradeshows..... A.6
training A.5
Transport
payload type.....7.15
transport
payload 7.19
TRIPWIRE_Attack.....C.56
turning off
scheduled reports w/o deleting...10.12
tutorials
counter-based attack signature 7.49
data-specific attack signature 7.40
network-specific attack signature ..7.45
overview 7.39

U

UDP
nonconnection-based attacks.....7.3
reserved keyword.....7.20
UDP Datagrams field..... 3.29, B.2
UDP header length. See UDP_MSG_LEN.
UDP header parameters 7.24
UDP-Scan.....C.56
UDP_DEST_ PORT
reserved keyword.....7.24
UDP_MSG_LEN
reserved keyword.....7.24
UDP_SMURF.....C.57
UDP_SRC_PORT
reserved keyword.....7.24
understanding
NetProwler 1.2
uninstalling NetProwler 2.11

Uninstalling the NetProwler Application dialog box 2.11
UNIX-Finger-Access-Decode C.57
UNIX-Finger-Bomb-Vulnerability.....C.58
UNIX-Hosts-File-Access C.58
UNIX-Rhost-File-Access C.59
UNIX_ADM_Messages_Attack C.61
UNIX_Aliases_Dir_Attack.....C.61
UNIX_Aliases_Pag_File_Attack C.62
UNIX_Bliss_Virus_Attack C.62
UNIX_CULOG_File_Attack C.63
UNIX_Errorlog_File C.63
UNIX_ETC_Exports_File_Attack C.64
UNIX_ETC_Host_File_Attack C.64
UNIX_ETC_Inetd_Conf_File_Attack ...C.65
UNIX_ETC_Utmp_File_Attack.....C.65
UNIX_Home_Change_Mode_Vulnerability C.60
UNIX_Host_Equiv_File_Attack.....C.66
UNIX_Loginlog_File_Attack.....C.66
UNIX_Mail_Change_Mode_Vulnerability C.60
UNIX_Passwd_File_Attack C.67
UNIX_Sulog_File_Attack.....C.67
UNIX_Var_Adm_Lastlog_File_Attack C.68
UNIX_XLOCK_Vulnerability C.68
Update both program files and configuration radio button..... 2.15
Update License
Administration menu option 3.6
Update program files, retain configuration radio button..... 2.15
updating
NetProwler's license..... 4.2
upgrading
NetProwler 2.13
urgent flag. See TCP_URG.
User Specified radio button
Profiler Schedule dialog box 5.15
Start Scan dialog box 5.5
user-defined 10.15
user-defined attacks
described 3.10
using
online help.....4.28

V

value primitives
building expressions with only one7.28
understanding 7.17
used in complex expressions.....7.29
used in simple expressions 7.28
viewing
a list of scheduled reports 10.11
alerts.....9.2
alerts by attack type 9.4
captured attack sessions.....9.5
captured conversations 9.11
comma-separated (CSV) reports..10.14
HTML reports.....10.13
live network sessions.....9.7
reports.....10.13
tab-separated (TSV) reports.....10.14
viewing captured sessions (tour).....3.32

W

Web Consistency Check dialog box.....8.3
Web Server Name list box.....8.3
Web Server Password field 8.3
Web server resources
deleting consistency check entries...8.6
modifying a consistency check entry8.5
securing.....1.8, 8.2
Web Server User field 8.3
Welcome dialog box.....2.8, 2.14

well-known port numbers 4.21
window size (in the TCP header). See
TCP_WINDOWSIZE.
Windows menu 3.7
Winnuke C.69
Word radio button
Value Primitives tab 7.18
WS_FTP_INI_Attack..... C.69

X

XOR operator..... 7.26
X_Server_Crash_Attack C.69

Y

year 2000 support..... A.4